Quinta-feira, 17 de junho de 2021

II Série
Número 96

BOLETIM OFICIAL

ÍNDICE

PARTE C

MINISTÉRIO DAS FINANÇAS

Direção Nacional da Administração Pública

Extrato do despacho nº 704/2021 — De S. Exª o Diretor Nacional da Administração Pública, por sub-delegação de competências da Secretária de Estado Adjunta para a Modernização Administrativa, através do Despacho nº 39/2018, de 16 de julho.

De 12 de abril de 2021:

José António Cabral Semedo, Subintendente da Policia Nacional, do quadro de pessoal do Ministério da Administração Interna, aposentado, nos termos do artigo 5º, nº 3, do Estatuto de Aposentação e da Pensão de Sobrevivência (EAPS), aprovado pela Lei nº 61/III/89, de 30 de dezembro, conjugado com a alínea a) do artigo 70º do Decreto-Legislativo nº 8/2010, de 28 de setembro, que aprova o Estatuto do Pessoal Policial da Polícia Nacional, com direito à pensão anual de 2.102.940,00 (dois milhões cento e dois mil novecentos e quarenta escudos), sujeita à retificação, calculada em conformidade com o artigo 37º do EAPS, correspondente a 34 anos de serviço prestado ao Estado, incluindo os aumentos legais.

A despesa tem cabimento no capitulo, 35.20, Divisão 04, Código 02.07.01.01.01 do orçamento vigente.

(Visado pelo Tribunal de Contas em 6 de maio de 2021)

Direção Nacional da Administração Pública do Ministério das Finanças, na Praia, 4 de junho de 2021. — O Diretor Nacional, *Mafaldo de Jesus Varela de Carvalho.*

Extrato do despacho nº 705/2021 — De S. Exª o Diretor Nacional da Administração Pública, por sub-delegação de competências da Secretária de Estado Adjunta para a Modernização Administrativa, através do Despacho nº 39/2018, de 16 de julho.

De 19 de março de 2021:

Rui Herculano Delgado, Técnico Auxiliar do quadro de pessoal da Câmara Municipal da Ribeira Grande - Santo Antão, aposentado, nos termos da alínea *b*) do nº 2 do artigo 5º do Estatuto de Aposentação e da Pensão de Sobrevivência (EAPS), aprovado pela Lei nº 61/III/89, de 30 de dezembro, com direito à pensão anual no valor de 493 332$00 (quatrocentos e noventa e três mil trezentos e trinta e dois escudos), sujeita à retificação, calculada em conformidade com o artigo 37º do EAPS, correspondente a 34 anos de serviço prestado ao Estado, incluindo os aumentos legais.

Esta pensão será dividida proporcionalmente da seguinte forma:

Orçamento do Estado……203.136$00

Por despacho de 14 de março de 2011 do Diretor Nacional do Orçamento da Contabilidade Pública, foi deferido o pedido de pagamento de quotas em atraso para compensação de aposentação, referente ao período de 17 anos, 7 meses e 28 dias.

O montante em dívida no valor de 286 516$00 (duzentos e oitenta e seis mil quinhentos e dezasseis escudos), será amortizado em 270 prestações mensais e consecutivas, sendo a primeira de 1 107$00 e as restantes de 1 061$00.

Orçamento da Câmara Municipal da Ribeira Grande- São Antão….290 196$00

A despesa tem cabimento no capitulo, 35.20, Divisão 04, Código 02.07.01.01.01 do orçamento vigente.

(Visado pelo Tribunal de Contas em 6 de maio de 2021)

Direção Nacional da Administração Pública do Ministério das Finanças, na Praia, 4 de junho de 2021. — O Diretor Nacional, *Mafaldo de Jesus Varela de Carvalho.*

PARTE E

ESTRADAS DE CABO VERDE

Despacho nº 4/2021

Ao abrigo do disposto no nº 2 do artigo 23º da Retificação à Portaria nº 5/2005, de 24 de janeiro, que aprova o Plano de Cargos Carreiras e Salário e o Regulamento de Avaliação de Desempenho do pessoal do Instituto de Estradas, agora Estradas de Cabo Verde, Entidade Pública Empresarial, progride os seguintes funcionários do quadro de pessoal da mesma empresa:

Maria Sábado da Veiga Semedo, enquadrada na Categoria de Auxiliar - Nível 101 progride par Auxiliar – Nível 102, com efeitos a partir de 6 de fevereiro de 2021.

Lenira Elisângela Ferreira Mendes da Costa, enquadrada na Categoria de Técnico Superior – Nível 102 progride para Técnico Superior – Nível 103, com efeitos a partir de 12 de maio de 2021.

Estradas de Cabo Verde, EPE na Praia, aos 15 de junho de 2021. — O Presidente do Conselho de Administração da ECV, EPE, *Eduardo Lopes.*

PARTE G

MUNICÍPIO DE SÃO DOMINGOS E INSTITUTO DO EMPREGO E FORMAÇÃO PROFISSIONAL

Câmara Municipal

Despacho conjunto nº 4/2021

12 de maio 2021

Agilson do Espírito Santos Ortet Licenciado em Economia e Gestão, Pessoal do Quadro do Instituto de Emprego e Formação Profissional Nível II, é nomeado em Comissão Serviço por substituição, para exercer o cargo do Director de Serviço do Gabinete de Estudos, Planeamento do Desenvolvimento Municipal, Conceção e Coordenação da Implementação de Projetos da Câmara Municipal de São Domingos, nos termos dos artigos 42º da Lei nº 42/VII/2009, de 27 de julho, que define as bases em que assenta o regime da Função Pública, conjugado com os artigos 33º e 47 do Decreto-lei nº 59/2014, de 4 de novembro, com efeitos a partir da publicação no *Boletim Oficial.*

Cidade de São Domingos aos 12 de maio de 2021

O Presidente da Camara Municipal, *Isaías Almeida Varela*

Presidente do Conselho Diretivo, *Paulo Alexandre Silva dos Santos.*

———o§o———

MUNICÍPIO DE SÃO DOMINGOS

Câmara Municipal

Deliberação nº 23/2021 — da Câmara Municipal de 3 de maio de 2021

Danielson Adérito Pereira Tavares, Técnico, Nível, I do Quadro de Pessoal da Câmara Municipal de São Domingos, dada por finda a comissão ordinária de serviço no cargo de Diretor de Serviços de Financeiros, nos termos previstos no nº 2, alínea *d*) do artigo 31º do Decreto-lei nº 59/2014, de 4 de novembro, com efeitos a partir do dia 1 de junho de 2021.

Câmara Municipal de São Domingos, aos 3 de maio de 2021. — Presidente da Câmara Municipal, *Isaías Almeida Varela.*

PARTE H

BANCO DE CABO VERDE

Gabinete do Governador e dos Conselhos

Relatório e Contas

Relatório e Contas do Fundo de Garantia de Depósito, referente ao ano de 2020

I. Introdução

O Fundo de Garantia de Depósitos foi criado a 27 de janeiro no âmbito da lei nº 7/IX/2017 e tem como finalidade proteger os depositantes no âmbito do sistema bancário, contribuir para a manutenção da estabilidade do sistema financeiro e mitigar os efeitos de uma eventual crise bancária.

A gestão do Fundo é assegurada por uma Comissão Diretiva, que foi indigitada nos termos do nº 2 do artigo 2º do Aviso nº 8/2017, de 3 de outubro. Compete-lhe efetuar, em nome e por conta e ordem do Fundo, todos os atos e operações necessários ou convenientes à realização do seu objeto.

II. Atividades desenvolvidas em 2020

1. Síntese das atividades do Fundo de Garantia de Depósitos

O ano de 2020 revelou-se um ano decisivo para o Fundo de Garantia de Depósitos nos domínios da realização de trabalhos, de natureza técnica e legal, não obstante as disrupções causadas pelo surto do coronavírus (COVID19) na atividade económica nacional.

No cumprimento da sua missão, o FGD, deu continuidade ao desenvolvimento de importantes atividades que são próprias de um sistema de garantia de depósitos com um regime contributivo de natureza ex-ante, de entre os quais:

- Cálculo do montante da contribuição anual devido por cada instituição participante o Fundo, relativo a 2020, que tem em conta os saldos médios dos depósitos abrangidos pela garantia no final de cada mês do ano de 2019, a taxa contributiva de base fixada pelo Banco de Cabo Verde e o fator de ajustamento ao risco para a instituição participante de acordo com o seu rácio médio de solvabilidade conforme Aviso 7/2019 de 3 de outubro e a Instrução Técnica nº 206, de 14 de fevereiro de 2020;

- Cobrança das referidas contribuições anuais e celebração com as instituições participantes de contratos de compromissos de pagamento, irrevogáveis, caucionados através dos títulos de dívida pública, pela parte daquelas contribuições não liquidadas em numerário até ao limite exigido pela Instrução Técnica a ser emitida pelo BCV;

- Aplicação dos recursos financeiros do Fundo, no quadro das diretrizes e dos princípios acordados com o Banco de Cabo Verde;

Para além daquelas atividades, o FGD desenvolveu ainda um conjunto de iniciativas relacionadas com os instrumentos de gestão financeira previsional destacando para o efeito a definição de um plano para mobilização de recursos financeiros para o biénio 2021-2022; a definição de um *benchmark* para a gestão da carteira de investimentos; e a definição da política de investimento que rege os investimentos do Fundo visando o cumprimento das suas finalidades de acordo com os critérios estabelecidos com o protocolo assinado com o Banco de Cabo Verde.

No domínio da organização interna do Fundo e da produção legal, o FGD concebeu o seu logotipo e participou na elaboração da Instrução Técnica que dispõe sobre a elaboração e fornecimento de informações relativas aos depósitos abrangidos pelo Fundo de Garantia de Depósitos.

Para concluir, um destaque especial à lei n.º 86/IX/2020 de 28 de abril que procede a republicação da lei nº 26/VIII/2013. Nesta lei, o artigo 29º vem estabelecer que ficam isentos de imposto sobre o rendimento, os rendimentos do Fundo de garantia de depósitos.

2. Apuramento do valor da Contribuição anual para o Fundo

O valor da contribuição anual de cada instituição participante é definido em função do valor médio dos saldos mensais dos depósitos do ano anterior garantidos pelo Fundo e do perfil de risco de cada instituição de crédito.

Nestes termos, ao valor médio em 2019 dos saldos dos depósitos cobertos, foi aplicado um fator multiplicador que resulta da ponderação da taxa contributiva de base através do rácio médio de solvabilidade calculado em base individual nos 2 últimos anos (artigo 4º do aviso nº 7/2019 que altera o Aviso nº 9/2017 de 3 de outubro).

As instituições participantes apresentaram em média rácios de solvabilidade acima dos 15%[1], e como consequência, por força do artigo 4º do aviso nº 7/2019 que altera o Aviso nº 9/2017 de 3 de outubro, a taxa contributiva de base aprovada pela Instrução Técnica n.º 206/2020 de 14 de fevereiro de 0,117%, foi objeto de um ajustamento calculado em função do perfil de risco recebendo as IP´s prémios de desconto diferenciados conforme norma vigente.

A observação do quadro 2 permite evidenciar as variáveis que tornaram possível o cálculo do valor da contribuição anual para o Fundo.

- Por um lado, tem-se a base de incidência que é o montante dos depósitos cobertos abrangidos pelo FGD, isto é, os depósitos de titulares elegíveis contabilizados até ao limite de 1.000.000 CVE; e

- Por outro, a taxa contributiva de base multiplicada por um fator de ajustamento calculado em função do perfil de risco de cada instituição participante, tendo em consideração a sua situação de solvabilidade.

O valor da Contribuição anual para o FGD em 2020 atingiu 59.413.416 CVE e foi apurado de acordo com a fórmula:

[1] Apenas duas instituições participantes do Fundo apresentaram um rácio de solvabilidade abaixo de 15%.

$$Valor\ de\ Contribuição\ (Ano\ n) = Dep.Cobertos(Ano\ n-1) \times Tx\ contrib.base \times Fator\ Ajust.ao\ Risco$$

Quadro 1

Apuramento do valor da contribuiçãopara o ano de 2020 (ECV)

	2019	2020
Depositos Cobertos no ano n-1 (1)	54 262 107 024	60 775 317 986
Tx Contributiva de base (2)	0,117%	0,117%
Fator Ajustamento ao Risco (3)	0,733	0,733
Valor da Contribuição paga pelas Instituições Participantes do FGD	**51 449 096**	**59 413 416**

(1) - Valor de dep. garantidos pelo FGD (i.e. depósitos de titulares elegíveis registados até ao limte de 1.000.000 ECV)

(2) - Taxa contributiva de base aprovada pela Instrução tecnica n.º 206/2020

(3) - Fator de ajustamento ao Risco = 12/RMS, em que o RMS é rácio medio de solvab. dos últimos 2 anos.

(Aviso 7/2019 que altera o Aviso 9/2017)

Regista-se que o valor da contribuição apurado e cobrado às IP's é ligeiramente superior ao resultado obtido pela fórmula acima indicada. Esta diferença obtida por excesso deve-se à cobrança do valor mínimo de contribuição a determinados Instituições que aquando da aplicação *da fórmula não alcançaram as contribuições mínimas* exigidas pelas instruções técnicas.

3. Contribuição das Instituições participantes para o Fundo

Feito o apuramento, o Banco de Cabo Verde notificou as IP´s do montante da respetiva contribuição anual, sendo que todas cumpriram integralmente as suas obrigações contributivas para o Fundo, no prazo e nas condições estabelecidas.

A 31 de dezembro de 2020, o valor da Contribuição anual atingiu CVE 164.647.476. A rubrica "Contribuições – Contratos de compromisso irrevogável" ascende a CVE 117.435.609, e as contribuições em numerário com CVE 47.211.867.

Quadro 2

Contribuições pagas pelas instituições participantes

Formas de pagamento utilizadas (CVE)

	2019	2020	Variação
Numerário	30 108 031	47 211 867	17 103 836
Compromissos irrevogaveis	75 126 029	117 435 609	42 309 580
Total	**105 234 060**	**164 647 476**	**59 413 416**

4. Recursos financeiros do Fundo

Os recursos próprios do Fundo alcançaram, no final do ano de 2020, CVE 199.521.374

Para a formação daquele valor concorreram:

- As contribuições periódicas das instituições participantes em numerário com CVE 47.211.867;
- As contribuições sob a forma de contratos de compromisso irrevogável com CVE 117.435.609;
- As coimas aplicadas às instituições participantes em CVE 30.941.233 resultantes do artigo 251º da Lei sobre as Atividades de Instituições Financeiras e o artigo 40º da Lei da Lavagem de Capitais que foram aplicadas no ano passado;
- Os CVE 1.493.687 relativos a resultados transitados; e
- E ainda os CVE 2.438.978 relativos a resultado líquido do Fundo.

Quadro 3

Recursos próprios

	2019	2020	Variação	
			Valor	%
Recursos Próprios	137 388 979	199 521 374	62 132 395	45,2%
1. Contribuições	105 234 060	164 647 476	59 413 416	56,5%
Contribuições iniciais	0	0	0	0
Contribuições anuais - realizadas	30 108 031	47 211 867	17 103 836	56,8%
Contribuições anuais - contratos de compromisso irrevogável	75 126 029	117 435 609	42 309 580	56,3%
2. Outras variações no capital próprio	30 661 233	30 941 233	280 000	0,9%
Produto de coimas aplicadas às IC	30 661 233	30 941 233	280 000	0,9%
4. Resultados	1 493 687	3 932 665	2 438 978	163,3%
Resultados transitados	415 199	1 493 687	1 078 488	n.d
Resultados líquido do período	1 078 488	2 438 978	1 360 490	126,1%

5. Target Fund Size

Considerando, que

- Os recursos próprios acumulados alcançados pelo Fundo em 2020, foi de CVE 199.521.374; e
- O montante total de depósitos cobertos pela garantia de reembolso do FGD (i.é depósitos de titulares elegíveis, contabilizados apenas até ao limite de CVE 1.000.000) foi de CVE 64.231.624.139.

Pode-se inferir que a relação entre os recursos próprios do Fundo e os depósitos efetivamente cobertos pela garantia em finais de dezembro de 2020 é de apenas 0,31%, um nível de capitalização que se situa ainda muito aquém do nível-alvo que se pretende atingir.

Quadro nº 4

Grau de cobertura dos Depósitos em 2020

Recursos próprios do Fundo (CVE)	199 521 374
Montante total de depósitos cobertos pela garantia do Fundo em 2020 (até 1.000.000 CVE)	64 231 624 139
Rácio	0,31%

Fonte: FGD

Recorde-se que no artigo 12º da lei 07/IX/2017 (nível-alvo do Fundo), o montante dos recursos financeiros disponíveis que o Fundo é obrigado a alcançar fixa-se em 5% do montante dos depósitos cobertos dos seus membros.

Distribuição dos depósitos, por intervalos de montantes depositados

A 31 de dezembro de 2020, no limite de CVE 1.000.000 encontra-se cobertos 93,5 por cento do número total de depositantes, e de 21,1 por cento do valor dos depósitos elegíveis.

Quadro nº 5

Distribuição dos depósitos, por intervalos de montantes depositados

Intervalos em função do saldo por depositante	% depositantes	% depósitos
De 0 a 1.000.000 CVE	93,5%	21,1%
Acima de 1.000.000 CVE	6,5%	78,9%

Fonte: FGD

6. Gestão Financeira do Fundo

- Enquadramento macroeconómico

O impacto transversal surto do coronavírus (COVID19) que teve início em dezembro de 2019 criou disrupções importantes para a atividade económica nacional e a dos seus parceiros económicos a um nível sem precedentes.

As medidas de políticas adotadas para contenção da propagação do novo coronavírus resultaram na contração do produto interno bruto (PIB) em volume do país na ordem dos 13 por cento em termos homólogos no primeiro semestre. As economias da Área do Euro, dos EUA e do Reino Unido - principais parceiros económicos do país - contraíram 9, 4 e 11 por cento, respetivamente, no primeiro semestre de 2020 face ao primeiro semestre de 2019.

As vulnerabilidades externas do país com a crise pandémica agravaram em larga medida. De acordo com a fonte do BCV, a balança corrente registou um défice de 11,4 por cento do PIB para o qual concorreu a queda de 39% das exportações de bens e serviços (que inclui as receitas de turismo e de transportes aéreos). Contudo, ao nível das contas externas, o *stock* das reservas internacionais líquidas tem-se mantido num nível relativamente confortável. De acordo com os dados do BCV, o stock cambial permitia, a 30 de junho, financiar 8.3 meses das importações de bens e serviços projetadas para 2020.

A par das vulnerabilidades externas, a crise pandémica exacerbou igualmente a posição das contas públicas. De acordo com o relatório de política monetária publicado pelo BCV em outubro de 2020, as contas públicas registaram um défice de 6.340 milhões de escudos em agosto de 2020, quase o dobro do défice registado no ano de 2019. Essa deterioração, segundo a mesma fonte, ficou a dever-se, principalmente, à queda das receitas fiscais (em 22,8 por cento), em particular de impostos sobre o valor acrescentado (22,7 por cento), sobre o rendimento de pessoas coletivas (43,1 por cento) e sobre as transações internacionais (16,3 por cento). A contribuição turística, por seu turno, reduziu 57 por cento, depois de ter crescido 1 por cento em 2019.

O défice das contas públicas foi financiado, maioritariamente, via emissão de obrigações de Tesouro, tanto junto a bancos como junto a outras entidades, à taxa média de 3,6 por cento (menos 0,4 pontos percentuais que a taxa média do período homólogo anterior). O endividamento externo, no quadro da ajuda orçamental e financiamento direto de projetos e medidas de alívio do impacto da pandemia no país, contribuiu, igualmente, em larga medida para o financiamento das necessidades do Estado.

O *stock* da dívida do governo central aumentou 9.421 milhões de escudos entre dezembro de 2019 e agosto de 2020, fixando-se em 264,2 biliões de escudos (146 por cento do PIB projetado para 2020). Em finais de 2019, a dívida do governo central fixava-se em 254,8 biliões de escudos (131 por cento do PIB). Excluindo os TCMF, a dívida do governo central fixava-se em 125 e 140 por cento do PIB, respetivamente, em dezembro de 2019 e agosto de 2020.

Não obstante o ciclo conturbado por que a passa a economia nacional, o sector monetário manteve-se líquido e o crédito ao sector privado aumentou 1,4 por cento entre dezembro de 2019 e agosto de 2020 (1,1 por cento entre dezembro de 2018 e agosto de 2019). Ao nível dos preços, a situação é estável. A inflação media anual medida pelo IPC situa-se nos 0.9 por cento em setembro de 2020, o que compara a 1,1 e 1,2 por cento registados respetivamente em setembro e dezembro de 2019.

- Gestão da carteira do FGD

No ano de 2020, o FGD manteve o elevado nível de prudência na gestão dos seus ativos financeiros em linha com um conjunto de critérios estabelecidos no protocolo que dispõe sobre diretrizes e os princípios que devem reger a gestão dos investimentos do Fundo de Garantia de Depósitos.

Nestes termos o Fundo participou em leilão competitivo referente ao ISIN CVOTEJOSG007, com maturidade a 02 de abril de 2023, no montante de CVE 46.000.000, tendo suportado uma comissão de corretagem, de CVE 115.000. A taxa de juro conseguida na OT fora de 3,4375%.

- O *benchmark* para a gestão da carteira de investimentos

Em dezembro de 2020, a Comissão Diretiva do FGD e o Conselho de Administração do Banco de Cabo Verde definiram como *benchmark* do FGD, a taxa média ponderada das emissões do Tesouro, que inclui as últimas 20 emissões de títulos de tesouro.

Essa taxa – denominada TOBIT – apresenta-se como parâmetro que visa acompanhar o desempenho de fundos de investimento em renda fixa prefixados, como é o caso do FGD que concentra a sua carteira em papéis com este perfil. Trata-se de uma solução que na ótica do FGD e do BCV, reflete não só o perfil de risco do fundo, com caráter essencialmente conservador, mas também, de fácil implementação e manutenção.

- Avaliação da performance do FGD face ao *benchmark* definido

Avaliando a performance do Fundo em 2020 pode-se afirmar que a gestão conseguiu superar a taxa média ponderada das emissões de tesouro das últimas vinte emissões de Obrigações (TOBIT).

O "Alfa"[2], diferença entre a performance do portfólio (ou ativo) em relação ao *Benchmark*, atingiu 1.1 sugerindo que o FGD superou o *benchmark* em 110%.

[2] **Alfa** é a diferença entre a performance do portfólio (ou ativo) em relação ao *Benchmark*. Isso é chamado de performance relativa. Ou seja, se o portfólio tiver um retorno maior, diz-se que o Alfa é positivo enquanto uma performance inferior indica um Alfa negativo.

Quadro n.º 6

Benchmark para o FGD

TOBIT = Taxa média ponderada das emissões do Tesouro

Ultimas 20 emissões

	2020
Taxa TOBIT	3,151%
Taxa de juro OT´s FGD	3,438%
Alfa (*)	1,1

(*) quando o "alfa" for superior a 1 estamos perante uma boa perfomance do FGD

7. Custos do Fundo

Não houve despesas de funcionamento no prosseguimento das atividades relacionadas com o Fundo. Ela assentou na colaboração a tempo parcial dos três elementos da Comissão Diretiva do Fundo, enquanto entidade gestora, e na disponibilização dos recursos humanos, técnicos e materiais assegurados pelo Banco de Cabo Verde, conforme o artigo 26.º da Lei 07/IX/17.

8. Diplomas e normativos publicados em 2020

1. Instrução Técnica n.º 206, de 14 de fevereiro de 2020, que fixa a taxa contributiva de base para 2020 em 0,117% e a contribuição anual mínima em 3.000.000 CVE;

2. Instrução técnica n.º 207, de 14 de fevereiro de 2020, que estabelece em 75% o limite do compromisso irrevogável de pagamento a aplicar nas contribuições de 2020;

3. Aviso n.º 10/2020 que altera o Aviso n.º 9/2017, de 3 de outubro, alterado e republicado pelo Aviso n.º 7/2019, de 13 de agosto;

4. Publicação do Relatório e Contas do FGD referente a 2019, no Boletim Oficial n.º 177, de 22 de dezembro de 2020;

5. Instrução Técnica anexa à Carta Circular Série "A", nº 210 de 03 de julho de 2020 que dispõe sobre a elaboração e fornecimento de informações relativas aos depósitos abrangidos pelo Fundo de Garantia de Depósitos;

6. Publicação da Lei n.º 86/IX/2020 de 28 de abril que procede a republicação da Lei n.º 26/VIII/2013 estabelecendo que ficam isentos de imposto sobre o rendimento, os rendimentos do Fundo de Garantia de Depósitos.

9. Apoio do Banco de Cabo Verde e a colaboração das Instituições participantes

A Comissão Diretiva do Fundo pretende expressar o seu reconhecimento a todas as unidades orgânicas do Banco de Cabo Verde que, de uma ou outra forma, contribuíram com os seus prestimosos apoios. Uma referência, em especial, ao Departamento de Contabilidade e Controlo Financeiro, ao Departamento de Mercados e Gestão de Reservas, ao Departamento de Supervisão Microprudencial e ao Gabinete do Governador e dos Conselhos.

Do mesmo modo, a Comissão Diretiva gostaria de exprimir o seu agrado pela colaboração sempre revelada pelas instituições participantes no seu relacionamento com o Fundo.

10. Nota final

Enumerados os aspetos considerados mais relevantes dos trabalhos realizados no âmbito do FGD ao longo do último ano, inclui-se a seguir e em anexo, toda a informação sobre a situação patrimonial do Fundo explicitada no seu balanço, ao qual se acrescentam algumas notas explicativas sobre o conteúdo das contas.

Banco de Cabo Verde, na Praia, aos 22 de janeiro de 2021

- Presidente, *Carlos Benoni de Brito Rezende Costa*

- Representante das instituições financeiras, *Maria de Fátima Jesus de Pina Veiga Pires*

- Representante do Banco de Cabo Verde, *Maria de Jesus Costa.*

III. Demonstrações financeiras e notas às contas

1. Demonstrações financeiras

FUNDO DE GARANTIA DE DEPÓSITOS

Quadro 7

Balanço a 31 de dezembro de 2020 e de 2019

Escudos cabo-verdianos

	Notas	31-dez-20	31-dez-19
ATIVO			
Ativo não corrente			
Investimentos financeiros		78.487.135	32.413.427
Outros investimentos financeiros	**3**	78.487.135	32.413.427
Instituições participantes		117.435.609	75.126.029
Contribuições - Contratos de compromisso irrevogável	**4**	117.435.609	75.126.029
Total do ativo não corrente		195.922.743	107.539.456
Ativo corrente			
Devedores por acréscimos de rendimentos	**5**	615.520	233.384
Outros devedores	**6**	0	0
Caixa e depósitos bancários	**7**	2.983.111	29.616.139
Total do ativo corrente		3.598.631	29.849.523
Total do ativo		**199.521.374**	**137.388.979**
CAPITAL PRÓPRIO E PASSIVO			
Capital próprio			
Contribuições realizadas	**8**	47.211.867	30.108.031
Contratos de compromisso irrevogável	**8**	117.435.609	75.126.029
Outras variações no capital próprio	**8**	30.941.233	30.661.233
Resultados transitados	**8**	1.493.687	415.199
Resultado líquido do período	**11**	2.438.978	1.078.488
Total do capital próprio		199.521.374	137.388.979
PASSIVO			
Passivo não corrente			
Total do passivo não corrente		0	0
Passivo corrente			
Total do passivo corrente		0	0
Total do passivo		**0**	**0**
Total do capital próprio e do passivo		**199.521.374**	**137.388.979**

Demonstrações financeiras e notas às contas

Demonstrações financeiras

FUNDO DE GARANTIA DE DEPÓSITOS

Quadro 8

Demonstração de Resultados do exercício findo em 31 de dezembro de 2020 e de 2019

Escudos cabo-verdianos

	Notas	31-dez-20	31-dez-19	Variação homóloga	
				Valor	%
Resultado de juros e de rendimentos e de gastos equiparados		2.454.812	1.128.488	1.326.324	117,5%
Juros recebidos	9	2.454.812	1.128.488	1.326.324	117,5%
Resultado da aplicação dos recursos disponíveis		**2.454.812**	**1.128.488**	**1.326.324**	**117,5%**
Outros gastos		15.834	50.000	-34.166	-68,3%
Resultado antes de provisões, imparidades, depreciações e amortizações, e impostos		**2.438.978**	**1.078.488**	**1.360.490**	**126,1%**
Resultado antes de impostos		**2.438.978**	**1.078.488**	**1.360.490**	**126,1%**
Resultado líquido do exercício	**11**	**2.438.978**	**1.078.488**	**1.360.490**	**126,1%**

FUNDO DE GARANTIA DE DEPÓSITOS

Quadro 9

Demonstração de alterações no Capital Próprio do exercício findo em 31 de dezembro de 2020 e de 2019

Escudos cabo-verdianos

	Periódicas		Resultados retidos	Outras variações no capital próprio	Resultado líquido	CAPITAL PRÓPRIO
	Realizadas	Contratos de compromisso irrevogável				
Posição a 31 de dezembro de 2018	**15.371.241**	**38.413.723**	**0**	**1.741.233**	**415.199**	**55.941.395**
Contribuições	**14.736.790**	**36.712.306**				**51.449.096**
Contribuições efetuadas pelas instituições participantes	14.736.790	36.712.306				51.449.096
Outras variações				**28.920.000**		**28.920.000**
Multa aplicada nos termos dos artigos 251º da LAF				28.920.000		28.920.000
Aplicação de resultados			**415.199**		**-415.199**	**0**
Resultado líquido do exercício					**1.078.488**	**1.078.488**
Posição a 31 de dezembro de 2019	**30.108.031**	**75.126.029**	**415.199**	**30.661.233**	**1.078.488**	**137.388.979**
Aplicação de resultados			**1.078.488**		**-1.078.488**	**0**
Contribuições	**17.103.837**	**42.309.580**				**59.413.416**
Contribuições efetuadas pelas instituições participantes	17.103.837	42.309.580				59.413.416
Outras variações				**280.000**		**280.000**
Multa aplicada nos termos dos artigos 251º da LAF				280.000		280.000
Resultado líquido do exercício					**2.438.978**	**2.438.978**
Posição a 31 de dezembro de 2020	**47.211.867**	**117.435.609**	**1.493.687**	**30.941.233**	**2.438.978**	**199.521.374**

FUNDO DE GARANTIA DE DEPÓSITOS

Quadro 10

Demonstração dos Fluxos de Caixa do exercício findo em 31 de dezembro de 2020 e de 2019

Escudos cabo-verdianos

	Notas	31-dez-20	31-dez-19
Fluxo e caixa das atividades operacionais			
Recebimento de contribuições		17.103.837	14.736.790
Outros recebimentos/pagamentos		280.000	28.920.000
FLUXO DE CAIXA DAS ATIVIDADES OPERACIONAIS		**17.383.837**	**43.656.790**
Fluxo de caixa das atividades de investimentos			
Pagamentos respeitantes a:			
Outros ativos		-46.115.000	-16.390.875
Aplicações em títulos da dívida pública caboverdiana		-46.115.000	-16.390.875
Recebimentos provenientes de:			
Juros e rendimentos similares		2.098.135	950.000
FLUXO DE CAIXA DAS ATIVIDADES DE INVESTIMENTO		**-44.016.865**	**-15.440.875**
Fluxo de caixa das atividades de financiamento			
Recebimentos provenientes de:			
Pagamentos respeitantes a:			
FLUXO DE CAIXA DAS ATIVIDADES DE FINANCIAMENTO		**0**	**0**
VARIAÇÃO DE CAIXA E SEUS EQUIVALENTES		**-26.633.028**	**28.215.915**
Caixa e seus equivalentes no início do exercício		29.616.139	1.400.224
Caixa e seus equivalentes no fim do exercício	**12**	2.983.111	29.616.139

2. **Notas às Demonstrações financeiras a 31 de dezembro de 2020 e de 2019**

(Valores expressos em escudos cabo-verdianos ou CVE)

NOTA 1 – NOTA INTRODUTÓRIA

O Fundo de Garantia de Depósitos (FGD ou Fundo) é uma pessoa coletiva de direito público criado pela Lei n.º 07/IX/2017, de 27 de janeiro, como elemento integrante do Sistema de Garantia preconizado no artigo 51º da Lei n.º 61/VIII/2014, de 23 de abril, que define as bases, os princípios orientadores e o quadro normativo de referência para o sistema financeiro Cabo-verdiano.

De acordo com o artigo 1º da Lei nº 07/IX/2017, o Fundo funciona junto do Banco de Cabo Verde que assegura os serviços técnicos e administrativos indispensáveis ao seu funcionamento.

O Fundo tem por objeto garantir o reembolso do valor global dos saldos em dinheiro de cada titular de depósito, até ao limite de CVE 1.000.000 (um milhão de escudos), de acordo com os limites e condições determinados nos artigos 7º a 9º da mesma Lei, na eventualidade de os depósitos das respetivas instituições participantes (artigo 4º) se tornarem indisponíveis, podendo, ainda, intervir no âmbito da execução de medidas de resolução, nos termos do artigo 166º e 171º da Lei n.º 62/VIII/2014, de 23 de abril.

Adicionalmente, informamos que as demonstrações financeiras são apresentadas em escudos Cabo-verdianos.

NOTA 2 – BASES DE APRESENTAÇÃO E PRINCIPAIS POLÍTICAS CONTABILÍSTICAS

2.1 Bases de apresentação

As demonstrações financeiras do Fundo de Garantia de Depósitos foram elaboradas e apresentadas de acordo com o seu Plano de Contas e seguem os princípios e orientações técnicas definidos pelo Sistema de Normalização Contabilística e de Relato Financeiro de Cabo Verde, aprovado pelo Decreto-Lei n.º 5/2008, de 04 de fevereiro, subsidiariamente pela Portaria nº 49/2008, de 29 de dezembro. Este plano define os modelos das demonstrações financeiras e o conteúdo de divulgação nas notas explicativas. Essas disposições específicas encontram-se devidamente assinaladas na Nota 2.2.

2.2 Resumo das principais políticas contabilísticas

As principais políticas contabilísticas e critérios valorimétricos utilizados na preparação das demonstrações financeiras do Fundo de Garantia de Depósitos com referência a 31 de dezembro de 2020 e de 2019 são os seguintes:

***a*) Pressupostos contabilísticos e características qualitativas das demonstrações financeiras**

As demonstrações financeiras do Fundo refletem a realidade económica dos seus ativos e passivos e são elaboradas de acordo com o Regime do Acréscimo (em relação à generalidade das rubricas das demonstrações financeiras, nomeadamente no que se refere aos juros das operações ativas e passivas que são registados à medida que são gerados, independentemente do momento do seu recebimento ou pagamento) e da Continuidade.

As características qualitativas das demonstrações financeiras são a Compreensibilidade, a Relevância, a Fiabilidade e a Comparabilidade.

***b*) Reconhecimento/desreconhecimento de ativos e passivos**

Os ativos são bens e direitos controlados pelo Fundo como resultado de acontecimentos passados dos quais se espera que fluam para a entidade benefícios económicos futuros. Os passivos são obrigações presentes da entidade provenientes de acontecimentos passados, cuja liquidação se espera que resulte numa saída ou aplicação de recursos incorporando benefícios económicos.

Os ativos e passivos são mensurados com fiabilidade e registados ao justo valor na data-valor, sendo que para aqueles não classificados na categoria de justo valor através do resultado, esse valor inclui todos os custos incorridos na operação. Esses ativos/passivos são desreconhecidos do balanço quando (i) os direitos/obrigações contratuais do Fundo relativos aos respetivos fluxos de caixa expiraram (ii) o Fundo transferiu substancialmente todos os riscos e benefícios associados à sua deteção ou, (iii) não obstante o Fundo ter retido parte, mas não substancialmente todos, os riscos e benefícios associados à sua deteção, o controlo sobre os ativos/passivos foi transferido.

***c*) Reconhecimento de resultados**

Os rendimentos e ganhos e os gastos e perdas são levados à conta de resultados nos períodos em que são gerados.

***d*) Mensuração dos elementos de balanço**

Os investimentos financeiros representam ativos financeiros detidos até à maturidade mensurados ao custo amortizado com base no método da taxa efetiva[3], sendo deduzidos de perdas de imparidade.

O custo amortizado é a quantia pela qual o ativo ou passivo financeiro é mensurado no reconhecimento inicial menos os reembolsos de capital mais ou menos a amortização cumulativa, usando o método de juro efetivo de qualquer diferença entre a quantia inicial e a quantia na maturidade, menos qualquer redução de imparidade.

As contribuições por realizar, as contas a receber e a pagar, caixa e depósitos junto de terceiros, assim como as restantes posições de balanço não referidas anteriormente, são reconhecidas ao valor nominal, deduzidas de eventuais perdas por imparidade.

***e*) Capitais Próprios**

Os recursos colocados à disposição do Fundo para o exercício da sua atividade englobam as contribuições a favor do Fundo efetuadas pelas instituições participantes e o produto das coimas aplicadas às instituições participantes nos termos da Lei.

(i) Contribuições e contratos de compromisso irrevogável

As instituições participantes entregam ao Fundo uma contribuição periódica fixada por Aviso do Banco de Cabo Verde, cujo valor é definido em função do volume de depósitos captados por cada instituição e a situação da sua solvabilidade.

De acordo com o artigo 14º da Lei nº 7/IX/2017, de 27 de janeiro, as instituições participantes poderão realizar esta contribuição em numerário ou serem dispensadas de efetuar o respetivo pagamento no prazo estabelecido, até ao limite de 75% (fixado anualmente pelo Banco de Cabo Verde) desde que assumam o compromisso, irrevogável e caucionado por penhor de valores mobiliários, de pagamento ao Fundo, em qualquer momento em que este o solicite, da totalidade ou de parte do montante da contribuição que não tiver sido pago em numerário. A parcela correspondente aos compromissos irrevogáveis de pagamento constitui também recursos do Fundo e é reconhecida por contrapartida de um ativo que é mensurado ao custo deduzido de perdas por imparidade.

[3] O método da taxa efetiva é o método de calcular o custo amortizado de um ativo ou passivo financeiro e de imputar o rendimento dos juros ou o gasto dos juros durante o período relevante. A taxa de juro efetiva é a taxa que desconta exatamente os pagamentos ou recebimentos de caixa futuros estimados durante a vida esperada do instrumento financeiro.

Em casos excecionais, as instituições participantes efetuam contribuições complementares previstas no artigo 15º da Lei n.º 07/IX/2017.

Através da Circular Série "A" nº 207, de 14 de fevereiro de 2020, o Banco de Cabo Verde fixou em 75% o limite do compromisso irrevogável a aplicar pelas instituições participantes nas contribuições referentes ao ano de 2020.

Pela Circular Série "A" nº 206, de 14 de fevereiro de 2020, o banco central fixou a taxa contributiva de base de cada instituição participante a vigorar no ano de 2020 em 0,117% sobre os depósitos cobertos e determinou a contribuição anual mínima a realizar pelas instituições participantes no ano de 2020 em CVE 3.000.000.

(ii) Coimas aplicadas pelo Banco de Cabo Verde cuja receita reverte a favor do FGD

De acordo com o artigo 14 da Lei n.º 07/IX/2017, de 27 de janeiro, as coimas aplicadas às instituições participantes no FGD resultantes de processos de contraordenação instaurados pelo Banco de Cabo Verde no exercício das suas funções de supervisão, nos casos em que a respetiva receita reverte a favor do FGD, são reconhecidas como Capital Próprio.

***f*) Caixa e equivalentes de caixa**

Na Demonstração de Fluxos de Caixa, o agregado "Caixa e seus equivalentes" agrega depósitos à ordem junto do banco central e das instituições de crédito no país.

***g*) Imposto sobre o rendimento**

Os recursos do Fundo foram aplicados em títulos do Tesouro, e como tal de acordo de com o artigo 24.º, n.º 1 do Código dos Benefícios Fiscais, "Os rendimentos das obrigações ou produto de natureza análoga, incluindo os títulos da dívida pública com colocação pública e cotados na Bolsa de Valores de Cabo Verde, são tributados em sede do imposto sobre o rendimento a uma taxa liberatória de 5%". No entanto ao abrigo do artigo 27.º . A aditado à Lei nº. 26/VIII/2013 a 28 de abril de 2020, os rendimentos do Fundo de Garantia de Depósitos, constituídos pelas instituições de crédito autorizadas a captar depósitos sujeitos à supervisão prudencial do Banco de Cabo Verde criado pela Lei n.º 7/IX/2017, de 27 de janeiro" ficam isentos de impostos sobre rendimento.

NOTA 3 – INVESTIMENTOS FINANCEIROS

Esta rubrica representa os títulos de dívida pública do Estado de Cabo Verde adquiridos pelo Fundo, no âmbito da sua política de investimentos e o tratamento contabilístico é o descrito na Nota 2.2, alínea *d*).

Quadro 11

Ativos financeiros detidos até à maturidade

Escudos cabo-verdianos

	31-dez-20	31-dez-19	Variação	
			Valor	%
Investimentos financeiros	78.487.135	32.413.427	46.073.707	142,1%
Obrigações do Tesouro	78.487.135	32.413.427	46.073.707	142,1%
Total investimentos financeiros	**78.487.135**	**32.413.427**	**46.073.707**	**142,1%**

Em 2020, o Fundo participou em leilão competitivo referente ao ISIN CVOTEJOSG007, com maturidade a 02 de abril de 2023, no montante de CVE 46.000.000, tendo suportado uma comissão de corretagem, de CVE 115.000.

NOTA 4 – CONTRIBUIÇÕES - CONTRATOS DE COMPROMISSO IRREVOGÁVEL

Representando 58,86% do Ativo, a rubrica evidencia o valor nominal dos compromissos irrevogáveis de pagamento assumidos pelas instituições de crédito participantes perante o Fundo, no âmbito das contribuições periódicas anuais, de acordo com a política contabilística descrita na Nota 2.2., alínea e) - (i).

Conforme previsto no Aviso nº 9/2017 do Banco de Cabo Verde, publicado no *Boletim Oficial* nº 52, de 3 de outubro de 2017, as instituições participantes tinham até o último dia útil de fevereiro de 2020 para pagarem ao Fundo a contribuição anual relativa ao ano de 2020.

Em finais de dezembro de 2020, o saldo da rubrica "Contribuições – Contratos de compromisso irrevogável" ascende a CVE 117.435.609 (2019: CVE 75.126.029) cerca de 56,32% acima do valor registado no início do ano e traduz o recebimento das contribuições de 2020. Estas ascendem a CVE 42.309.580, um crescimento de 15,25% face ao início do ano e repercute o aumento dos depósitos cobertos. De realçar que, no exercício foi efetuada a correção da contribuição feita em 2018, no valor de CVE 574.000, devido à alteração da base de incidência para o apuramento do valor da contribuição das instituições participantes (depósitos cobertos).

NOTA 5 – DEVEDORES POR ACRÉSCIMOS DE RENDIMENTOS

A 31 de dezembro de 2020, esta rubrica do ativo ascende a CVE 615.520 (2019: CVE 233.384), e compreendia os juros especializados das Obrigações do Tesouro classificados na categoria de ativos detidos até à maturidade. Estes ativos vencem juros a taxas nominais que variam entre 3,4375% a 4,375% e com a maturidade entre 2021 a 2028.

NOTA 6 – OUTROS DEVEDORES

Registam-se nesta rubrica os valores a receber que aguardam regularização. No final do exercício de 2020, o saldo é nulo e reflete a normalização do valor pendente em maio de 2020.

NOTA 7 – CAIXA E DEPÓSITOS BANCÁRIOS

A rubrica releva o montante em depósitos à ordem no Banco de Cabo Verde e nas instituições de crédito no país. A 31 de dezembro de 2020, os depósitos bancários totalizam CVE 2.983.111, sendo CVE 355.101 junto do Banco de Cabo Verde e CVE 2.628.010 junto das instituições de crédito.

No exercício, o Fundo recebeu juros da carteira de investimentos financeiros, no valor de CVE 2.113.969 (2019: 1000.000) tendo suportado imposto de capital, de CVE 15.834.

De realçar, ainda, o recebimento de CVE 280.000, proveniente da coima aplicada pelo BCV que reverte a favor do Fundo, ao abrigo dos artigos 251º da Lei nº. 62/VIII/2014, de 23 de abril que regula a atividade financeira com sede em Cabo Verde e a devolução de CVE 190.690, relacionada com a correção da contribuição de 2018, decorrente da alteração da base de incidência para o apuramento do valor da contribuição das instituições participantes (depósitos cobertos).

NOTA 8 – CAPITAL PRÓPRIO

O Capital Próprio do Fundo é constituído pelas contribuições periódicas das instituições de crédito participantes, pelo produto das coimas aplicadas às instituições participantes, nos termos da lei, pelos resultados transitados e pelo resultado do período. A composição e as variações desta rubrica são apresentadas na Demonstração de alterações no Capital Próprio.

No final de dezembro de 2020, as contribuições periódicas realizadas em numerário pelas instituições participantes no Fundo atingem CVE 47.211.867 (2019: CVE 30.108.031), enquanto os contratos de compromissos irrevogáveis das instituições participantes ascendem a CVE 117.435.609 (2019: 75.126.029) , de acordo com a política contabilística descrita na Nota 2.2., alínea *e*) – (i).

De realçar, a correção da contribuição de 2018, de CVE 764.690, associada à alteração da base de incidência para o apuramento do valor da contribuição das instituições participantes (depósitos cobertos).

A rubrica agrega, ainda, o valor de CVE 30.941.233 (2019: 30.661.233) resultante da coima aplicada às instituições participantes, conforme descrito na Nota 2.2, alínea *e*) – (ii), o resultado transitado no montante de CVE 1.493.687 positivos (2019: CVE 415.199) e o resultado líquido do exercício, de CVE 2.438.978 positivos, (2019: CVE 1.078.488) apurado conforme a Nota 2.2, alínea c). A composição e as variações do resultado do exercício são apresentadas na Demonstração de resultados do Fundo.

A composição do capital próprio do Fundo de Garantia de Depósitos a 31 de dezembro de 2020 e de 2019 é a que se apresenta:

Quadro 12

Composição do Capital Próprio

Escudos cabo-verdianos

	31-dez-20	31-dez-19
Capital próprio		
Contribuições realizadas	47.211.867	30.108.031
Contratos de compromisso irrevogável	117.435.609	75.126.029
Outras variações no capital próprio	30.941.233	30.661.233
Resultados transitados	1.493.687	415.199
Resultado líquido do exercício	2.438.978	1.078.488
Total do capital próprio	**199.521.374**	**137.388.979**

NOTA 9 – RESULTADO DE JUROS E DE RENDIMENTOS E DE GASTOS EQUIPARADOS

Esta rubrica agrega os juros reconhecidos da carteira de títulos detidos até à maturidade que no período ascende o valor de CVE 2.454.812 (2019: CVE 1.128.488).

NOTA 10 – OUTROS GASTOS

No montante de CVE 15.834, representa o imposto de capital cobrado sobre os juros recebidos da carteira de investimentos financeiros até março de 2020, em decorrência do aditamento do artigo 27.º A à Lei nº. 26/VIII/2013 a 28 de abril de 2020, que estabelece que os rendimentos do Fundo de Garantia de Depósitos, constituídos pelas instituições de crédito autorizadas a captar depósitos sujeitos à supervisão prudencial do Banco de Cabo Verde criado pela Lei nº 7/IX/2017, de 27 de janeiro" estão isentos de impostos sobre rendimento.

NOTA 11 – RESULTADO DO EXERCÍCIO

A 31 dezembro de 2020, o resultado líquido do exercício ascende a CVE 2.438.978, (2019: CVE 1.078.488) determinado pelo resultado da aplicação dos recursos do Fundo, conforme descrito na Nota 9, e encargos suportados, de acordo com a Nota 10.

NOTA 12 – CAIXA E EQUIVALENTES DE CAIXA

O objetivo da Demonstração de Fluxo de Caixa é evidenciar a capacidade de uma entidade gerar caixa para fazer face às suas necessidades de liquidez. Na Demonstração de Fluxo de Caixa, o *item* "Caixa e Equivalentes de Caixa" compreende as disponibilidades junto de instituições financeiras.

NOTA 13 – CONTAS EXTRAPATRIMONIAIS

Em finais de dezembro de 2020, as contas extrapatrimoniais apresentam a seguinte discriminação:

Quadro 13

Garantias dos contratos de compromissos irrevogáveis de pagamento

Escudos cabo-verdianos

	31/12/2020	31/12/2019
Garantias recebidas	117.435.609	75.126.029
Contrapartidas	117.435.609	75.126.029

A rubrica "Garantias recebidas" retrata valores mobiliários recebidos em caução - Títulos da dívida Pública do Estado de Cabo Verde como garantia do compromisso irrevogável de pagamento firmado com as instituições participantes no Fundo, conforme a Nota 4. Os valores mobiliários recebidos são registados conforme a política contabilística descrita na Nota 2.2., alínea *e*) - (i).

NOTA 14 – PARTES RELACIONADAS

Assente no artigo 19º da Lei n.º 07/IX/2017, de 27 de janeiro, o Fundo de Garantia de Depósitos é gerido por uma Comissão Diretiva composta por três membros conforme o aviso nº. 8/2017 do Banco de Cabo Verde, publicado no *Boletim Oficial* nº 52, de 03 de outubro de 2017, sendo dois membros em representação do Banco de Cabo Verde, dos quais um exerce o cargo de Presidente do Fundo e um membro em representação das instituições participantes.

Banco de Cabo Verde, na Praia, aos 22 de janeiro de 2021

- Presidente, *Carlos Benoni de Brito Rezende Costa*

- Representante das instituições financeiras, *Maria de Fátima Jesus de Pina Veiga Pires*

- Representante do Banco de Cabo Verde, *Maria de Jesus Costa.*

Aviso nº 1/2021

Gestão, processamento de operações e anomalias em rede partilhada de pagamentos com cartão ou dispositivo semelhante

Uma rede partilhada de pagamentos, doravante rede, possibilita ao utilizador de instrumento de pagamento, entre os quais cartão de pagamento ou dispositivo semelhante, conectar-se com diferentes intervenientes de um sistema e aceder a um leque diversificado de serviços de pagamento eletrónicos, seja no comércio físico, na *internet* ou por meio de qualquer dispositivo conectado à respetiva rede. A tecnologia associada a uma rede permite executar operações com segurança e conforto, fora de horários normais de funcionamento e do balcão de domiciliação.

No âmbito do acompanhamento da única rede partilhada de pagamentos com cartão existente no país, até o momento, o Banco de Cabo Verde (BCV) tem deparado com algumas situações devido a ocorrência de anomalias operacionais, nomeadamente pela troca de cacifos nos caixas automáticos (ATM), retenção anormal de cartão, falhas na entrega de notas nas operações de levantamentos de numerário, não concretização de uma transferência ou pagamento de bens e serviços cujo valor foi entretanto debitado da conta de pagamento do titular, inoperacionalidade de caixa automático ou terminal de pagamento automático (POS), entre outras, que podem materializar-se, ainda que temporariamente, em benefícios ou prejuízos para as partes envolvidas na operação de pagamento.

Assim, atendendo ao papel que lhe cabe que deve "*assegurar diretamente ou regular, fiscalizar e promover o bom funcionamento dos sistemas de compensação e pagamentos",* nos termos definidos no artigo 19.º da sua Lei Orgânica (Lei n.º 10/VI/2002, de 15 de julho, alterada pela Lei n.º 84/IX/2020, de 4 de abril), e no uso da competência que lhe confere o artigo 69.º do Decreto-legislativo n. º 8/2018, de 28 de novembro, o BCV aprova o presente Aviso com o fito de estabelecer as condições gerais de realização de operações numa rede, bem como normalizar o processo de regularização das anomalias, especialmente no que toca à imputação de responsabilidades aos diversos intervenientes do sistema, sempre que tal se mostrar necessário.

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

O presente Aviso estabelece as regras que devem ser observadas no funcionamento da rede, incluindo a regularização de anomalias operacionais, define os deveres dos participantes e utilizadores e, bem assim, os prazos para a regularização das principais anomalias.

Artigo 2º

Âmbito de aplicação

1. O presente Aviso aplica-se aos intervenientes numa rede, quais sejam, operadores de rede, prestadores de serviços de pagamento (PSP), utilizadores de instrumentos de pagamento afetos à rede e outras entidades autorizadas ou que venham a ser autorizadas, nos termos da legislação aplicável, a participar numa rede;

2. Para efeitos do número anterior, consideram-se PSP, designadamente:

a) As instituições de crédito;

b) As instituições de pagamento;

c) As instituições de moeda eletrónica; e

d) Outras que como tal sejam qualificadas pela lei.

Artigo 3.º

Definições

Para os efeitos do presente Aviso, entende-se por:

a) «Aceitante» toda e qualquer entidade que aceita o pagamento de bens ou serviços com um cartão de pagamento ou dispositivo semelhante e que mantém com um adquirente um contrato quadro para a realização deste serviço;

b) «Âmbito restrito» todo o cartão de pagamento ou dispositivo semelhante cuja utilização é limitada à realização de pagamentos de bens e serviços a um comerciante específico ou a um conjunto restrito de comerciantes associados sob um mesmo nome, marca e/ou logotipo, aprovado como tal pelo Banco de Cabo Verde;

c) «Anomalia» toda e qualquer falha operacional numa rede que possa traduzir-se, ainda que temporariamente, em benefícios ou prejuízos para a(s) parte(s) envolvida(s) na operação de pagamento;

d) «Adquirente (*acquirer*)» um PSP vinculado por contrato quadro a um comerciante para aceitar e processar operações de pagamento baseadas em marca de cartão ou dispositivo semelhante que representa, as quais dão origem a uma transferência de fundos para o comerciante. O adquirente assegura o pagamento (isto é, adquire o crédito) ao comerciante e é reembolsado pela entidade emitente do cartão ou responsável pela prestação de serviços de pagamento acessíveis através de dispositivo semelhante do utilizador;

e) «ATM de acesso restrito» equipamento automático pertencente a um PSP e que permite aos titulares de cartões emitidos por esse mesmo PSP, e só esses, realizar operações de pagamento, sem a necessidade de recorrer aos balcões. Tais equipamentos têm acesso interno às agências ou dependências de prestação de serviços de pagamento do PSP, durante o horário normal de funcionamento desse ou, senão, mediante uma autorização especifica;

f) «Caixa automático (ATM)» equipamento automático de uma rede do sistema de pagamentos, que permite aos titulares de cartões de pagamento ou dispositivo semelhante realizar diversas operações de pagamento, sem a necessidade de recorrer aos balcões dos prestadores de serviços de pagamento;

g) «Cartão de pagamento» instrumento de pagamento, geralmente sob a forma de cartão de plástico, emitido por um prestador de serviços de pagamento (instituições de crédito, instituições de pagamento ou instituições de moeda eletrónica) devidamente autorizado, que o disponibiliza ao titular, por via de um contrato quadro, para, de entre outras operações, efetuar pagamentos de bens ou serviços nos terminais de pagamento automático existentes nos pontos de venda aceitantes e à distância, por exemplo através da *internet*;

h) «Cliente» pessoa que contacta o emitente para contratar a emissão de cartão de pagamento ou a prestação de serviços de pagamento através de dispositivo semelhante;

i) «Comerciante» conceito que, ao fazer referência a cartões de pagamento ou dispositivo semelhante, designa genericamente todos os estabelecimentos comerciais, empresas, serviços ou profissionais liberais que aceitam pagamento por cartão ou dispositivo semelhante;

j) «CVV2» (*Card Verification Value*) código de verificação de 3 dígitos impresso no verso do cartão, à direita do painel da assinatura, após o número de conta pessoal. Trata-se de um dispositivo de autenticação de forma a evitar fraude na utilização de cartões em ambientes não controlados ou com cartão não presente tais como, telefone, correio ou *internet*;

k) «Entidade processadora» entidade responsável por receber e processar as operações necessárias ao funcionamento do sistema de compensação, prestando os correspondentes serviços às instituições participantes nesse sistema;

l) «Emitente» prestador de serviços de pagamento autorizado pelo Banco de Cabo Verde que emite cartões de pagamento (crédito, débito ou pré-pago), nos termos da legislação aplicável. Nos casos dos dispositivos semelhantes, é a entidade que presta serviços de pagamento através desses, nos termos da legislação aplicável. Nos sistemas de moeda eletrónica (pré-pago ou de valor armazenado) é a entidade que recebe os pagamentos em troca do valor distribuído no sistema e que está obrigada a pagar as transações ou a redimir os saldos que lhe são apresentados;

m) «*Host*» expressão que, em linguagem informática, significa qualquer máquina ou computador conectado a uma rede e que é identificado por um nome e um IP (número único);

n) «Instituição de apoio» prestador de serviços de pagamento que se responsabiliza pelas condições de instalação e de suporte logístico aos terminais de pagamento automático e caixas automáticos, mais concretamente, pelo abastecimento de notas e papel para impressão de recibos;

o) «Instituição de crédito» instituição financeira que, além de outras atividades financeiras, exerce a atividade de concessão de crédito, listadas na alínea a) do número 2, do artigo 20.º da Lei de Bases do Sistema Financeiro;

p) «Instituição de moeda eletrónica» pessoas coletivas a quem tenha sido concedida autorização, nos termos do artigo 11.º do Decreto-legislativo n.º 9/2018, de 28 de novembro;

q) «Instituição de pagamento» pessoas coletivas a quem tenha sido concedida autorização, nos termos do artigo 11.º do Decreto-legislativo n.º 9/2018, de 28 de novembro;

r) «Instituição financeira» pessoa ou entidade, singular ou coletiva, pública ou privada, legalmente autorizada pelo Banco de Cabo Verde a exercer uma ou mais atividades financeiras, listadas no número 2 do artigo 20.º da Lei de Bases do Sistema Financeiro;

s) «Instrumento de pagamento» qualquer dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador de serviço de pagamento e a que o utilizador de serviços de pagamento recorra para emitir ordem de pagamento;

t) «Lista negra» lista contendo números, ou séries de números, de cartões suspeitos existentes num sistema de cartões de pagamento e acessível a partir do terminal do comerciante. Serve para detetar ou bloquear qualquer transação efetuada pelos cartões nela incluídos;

u) «Manual de funcionamento» instrumento regulador das relações existentes entre as instituições participantes numa rede e respetivo operador, que contém a descrição dos processos e aspetos técnicos necessários à implementação dos diferentes serviços prestados pela rede;

v) «Operador de rede» entidade responsável pela gestão da base de dados de terminais de uma rede e pelo funcionamento e autenticação dos caixas automáticos e dos terminais de pagamento automático onde se realizam transações com cartão ou dispositivo semelhante;

w) «Participante» qualquer entidade que participe num serviço prestado por uma rede, tais como, emitente, adquirente, instituição de apoio e empresa prestadora de serviço;

x) «PC» sigla inglesa para computador pessoal;

y) «PIN» (*Personal identification number*) código numérico, pessoal e secreto do instrumento de pagamento do titular para fins de identificação em transações com cartão ou dispositivo semelhante;

z) «POS» (*Point of sale*) terminal de pagamento automático (TPA) instalado nos estabelecimentos comerciais que permite a utilização de cartão ou dispositivo semelhante;

aa) «Prestador de serviços de pagamento (PSP)» entidade autorizada a exercer a atividade de prestação de serviços de pagamento a título profissional, nos termos da legislação aplicável e respetiva regulamentação do Banco de Cabo Verde;

bb) «Rede» rede partilhada de pagamentos que permite ao utilizador de cartão de pagamento ou dispositivo semelhante, o acesso à sua conta de pagamento e a realização de operações em caixas automáticos e terminais de pagamento automático;

cc) «*Scheme*» conjunto de regras e procedimentos que norteia a prestação de um determinado serviço de pagamento ao público. São exemplos os procedimentos utilizados para realizar compras com cartões de crédito, débito e pré-pago, seja em moeda nacional ou em moeda estrangeira;

dd) «Serviços *web* (*internet*) e *mobile* (telemóvel)» serviços que dão ao cliente de um prestador de serviços de pagamento a possibilidade de aderir e aceder a uma rede e realizar operações de pagamento relativamente às contas de que seja único titular, ou cotitular, e que possa livremente movimentar. Esses serviços permitem ao cliente, através de um único acesso, aceder a diversas contas que detenha num mesmo prestador de serviços de pagamento ou em vários prestadores de serviços de pagamento;

ee) «SPI» sistema de pagamentos internacionais de cartões, identificáveis pelas respetivas marcas;

ff) «Supervisor» pessoa indicada pela instituição de apoio, responsável pela monitorização, seguimento e gestão operacional de caixa automático, que o operador da rede possa contactar sempre que se revelar necessário e que intervenha junto de ATM, quando solicitado;

gg) «Talão» documento prova da operação realizada com recurso a cartão de pagamento ou dispositivo semelhante. De entre outros elementos, normalmente ele contém os dados do terminal onde a transação foi realizada e o número do cartão. No caso concreto dos TPA, inclui ainda a identificação do comerciante onde a operação teve lugar. Por razões de segurança, é normal o número de cartão ou dispositivo semelhante aparecer parcialmente omisso;

hh) «Terminal de acesso à rede» equipamento automático de uma rede de pagamentos (caixa automático, TPA ou outro) que permite aos titulares de cartões de pagamento ou dispositivo semelhante realizar diversas operações de pagamento. Ver definições de "Caixa automático" e "Terminal de pagamento automático";

ii) «Terminal de pagamento automático (TPA)» o mesmo que *Point of Sale* (POS);

jj) «Transações fraudulentas» operações de pagamento em que o utilizador/titular de cartão de pagamento ou dispositivo semelhante não consentiu na sua execução, portanto, que se consideram não autorizadas e suscetíveis de originar uma reclamação;

kk) «Utilizador» pessoa singular ou coletiva que utiliza uma rede, para realização de operações de pagamento, de acordo com os termos e condições estabelecidos num contrato quadro.

Artigo 4.º

Contrato de subscrição de serviços de uma rede

À subscrição de serviços de uma rede aplicam-se as regras relativas aos contratos quadro, previstas na Secção III do Capítulo I do Título II do Decreto-legislativo n.º 8/2018, de 28 de novembro que estabelece o regime jurídico dos serviços de pagamento e da emissão, distribuição e reembolso de moeda eletrónica.

Artigo 5.º

Compensação de operações com cartão ou dispositivos semelhantes

1. Os requisitos de participação no sistema de compensação de operações com cartão ou dispositivo semelhante devem ser objetivos, públicos e não discriminatórios.

2. O sistema de compensação de operações com cartão ou dispositivo semelhante engloba as operações realizadas nos terminais com acesso a cada rede – quais sejam, caixa automático (ATM), *point of sale* (POS), *Web* (*internet*) e *mobile* (telemóvel), em conformidade com os procedimentos estabelecidos pelo *scheme* de pagamentos de cada rede.

3. Todas as operações financeiras que têm lugar numa determinada rede, independentemente do tipo de cartão ou dispositivo semelhante e do emitente, devem ser incluídas na compensação de operações com cartão ou dispositivo semelhante.

4. Excluam-se do disposto no número anterior os cartões de âmbito restrito.

5. Para efeitos de compensação, liquidação definitiva e finalização de pagamento, o processamento das operações no sistema é exclusivamente em escudos cabo-verdianos, ainda que a moeda da conta de pagamento que esteja associada ao cartão ou dispositivo semelhante seja outra que não a nacional.

6. O operador de rede é responsável:

a) Por providenciar a certificação dos equipamentos da respetiva rede para a aceitação das marcas de cartões nacionais e internacionais;

b) Por providenciar a certificação do *host* bancário do adquirente e emitente de operações na rede;

c) Por disponibilizar um serviço de prevenção, deteção e controlo de fraude, visando impedir a ocorrência de fraudes ou, pelo menos, mitigar o seu impacto, sendo que:

i. A concretização do serviço deve ser baseada num manual de normas e procedimentos a submeter pelo operador da rede ao Banco de Cabo Verde, para aprovação;

ii. O manual de normas e procedimentos suprarreferido deve ser atualizado sempre que as partes acharem conveniente, inclusive nas situações em que houver alterações de natureza regulamentar ou tecnológica;

iii. O serviço deve ser prestado a todos os PSP participantes da rede e implementado nas vertentes de emissão e de aceitação.

7. Antecipando-se a introdução de qualquer novo serviço prestado no sistema do serviço da rede, deve o operador executar os seguintes procedimentos:

a) Apresentar ao Banco de Cabo Verde o manual de funcionamento do serviço, incluindo o respetivo modelo de negócio, para avaliação do seu enquadramento;

b) Divulgar o manual de funcionamento a todos os participantes;

c) Disponibilizar informação documentada aos participantes sobre os procedimentos relacionados com o acesso técnico dos mesmos ao sistema.

8. A compensação multilateral das operações com cartão ou dispositivo semelhante, realizadas em território nacional, independentemente da marca de cartão, deve ser processada por uma entidade designada pelo Banco de Cabo Verde e nos termos da regulamentação desse sistema.

Artigo 6.º

Regras de funcionamento de uma rede

1. Todos os ATM com acesso externo às agências ou dependências de prestação de serviços de pagamento ou com disponibilização de serviços fora do horário de funcionamento normal das mesmas devem integrar uma rede partilhada.

2. Todos os POS suscetíveis de serem utilizados por cartões de pagamento ou dispositivo semelhante que não sejam de âmbito restrito devem integrar uma rede partilhada.

3. A aceitação em Cabo Verde de cartões de pagamento ou dispositivo semelhante que não sejam de âmbito restrito só se pode verificar em terminais de uma rede partilhada ou em ATM de acesso restrito, criadas em conformidade com o disposto no número 1, do presente artigo, sendo que:

a) A aceitação de cartões de pagamento em caixas automáticos que não estejam integrados numa rede partilhada implica o acordo prévio do operador de rede, enquanto administrador do *scheme* de pagamentos dessa rede;

b) Nos ATM de acesso restrito apenas devem ser aceites cartões emitidos ou dispositivos semelhantes do próprio PSP responsável pelo ATM.

4. A aceitação de cartões ou dispositivo semelhante de âmbito restrito nos terminais de uma determinada rede pressupõe a certificação destes cartões ou dispositivo semelhante pelo operador e a recolha de informação estatística sobre essa utilização, conforme definido pelo Banco de Cabo Verde.

5. O operador deve estabelecer regras de funcionamento que incentivem a expansão da sua rede a todas as ilhas do arquipélago e garantir o acesso da população aos seus serviços.

6. Desde que a marca e o tipo de cartão ou dispositivo semelhante sejam aceites no terminal, os serviços disponíveis numa determinada rede, designadamente nos ATM e POS, são independentes quer da instituição de apoio, bem como do emitente.

7. Os serviços de levantamento disponíveis numa rede, nomeadamente nos ATM, podem ser efetuados sem cartão, observando os procedimentos determinados pelo *scheme* de pagamentos da rede.

Artigo 7.º

Sistemas de pagamentos internacionais (SPI)

1. Uma instituição financeira não necessita de autorização específica do Banco de Cabo Verde para a respetiva filiação num SPI, observando-se o seguinte:

a) A instituição financeira em causa é participante numa rede cujo operador seja adquirente do SPI em causa;

b) A filiação no SPI não tem carácter de exclusividade em Cabo Verde, exceto em casos em que tal seja exigido pelo SPI e sujeitos a autorização pelo Banco de Cabo Verde, caso a caso;

c) As condições para a aceitação dos cartões do SPI em qualquer ATM integrado numa rede são determinadas pelo operador dessa rede;

d) No caso dos POS, a aceitação de cartões do SPI nesses terminais implica previamente a celebração de um acordo entre o respetivo comerciante e uma instituição financeira filiada no SPI.

2. As instituições financeiras emitentes ou adquirentes de cartões de SPI devem utilizar os serviços de processamento da entidade processadora indicada pelo Banco de Cabo Verde:

a) Caso a entidade processadora, com conhecimento do Banco de Cabo Verde, declare formalmente não estar habilitada a processar determinada marca de cartões de pagamento, desenvolver um dado produto ou executar certas funcionalidades, as instituições financeiras ficam autorizadas a utilizar os serviços de processamento de terceiros;

b) A autorização concedida de acordo com a alínea anterior expira 24 (vinte e quatro) meses após a entidade processadora indicada pelo Banco de Cabo Verde declarar reunir as condições para processar a marca, desenvolver o produto ou executar as funcionalidades em causa.

3. Qualquer rede a operar em Cabo Verde deve envidar esforços no sentido de se certificar para a aceitação de cartões dos SPI.

CAPÍTULO II

RESPONSABILIDADES DOS INTERVENIENTES

Artigo 8.º

Gestão do sistema

1. Cabe ao operador de rede:

a) Gerir a sua rede de ATM, responsabilizando-se pela qualidade do serviço e segurança do sistema, e para tal deve responder:

i. Pelo horário de funcionamento do sistema, salvo situações técnicas de exceção, tais como falhas das linhas de comunicação da responsabilidade do provedor de telecomunicações e ataques cibernéticos;

ii. Pelas operações disponíveis na rede, podendo restringir ou alargar a sua utilização como resultado da combinação "horários de utilização-afluência de utilizadores-operações essenciais";

iii. Pela deteção de anomalias, devendo entrar em contato com o supervisor encarregado da supervisão do ATM em causa, para reporte da ocorrência e, eventualmente, solicitar uma intervenção junto do equipamento, a fim de repor o seu normal funcionamento num período máximo de 48 (quarenta e oito) horas;

iv. Contactar o pessoal encarregado de assistência dos circuitos e/ou equipamentos, no caso da anomalia não ser ultrapassada pela intervenção do supervisor da agência.

b) Gerir a rede de pagamentos automáticos, no que toca à gestão:

i. Da infraestrutura de suporte que assegura a comunicação do sistema com a rede de POS e com os sistemas dos PSP;

ii. Do centro de apoio ao comerciante e aos PSP;

iii. Da rede de comerciantes.

c) Garantir que:

i. Uma mensagem visível no ecrã do ATM, ou uma gravação de voz, alerte os utilizadores para a retirada do seu cartão, a fim de minimizar as situações em que a máquina retém o cartão por esquecimento do utilizador;

ii. Os ATM dispõem da função de retenção de cartão em caso de incidentes, nomeadamente esquecimento de cartão na ranhura da máquina, uso de cartões expirados, bloqueados ou denunciados, e introdução errada do PIN por mais de três vezes consecutivas;

iii. Os contactos do centro de atendimento são corretamente exibidos nos ATM da rede. No mínimo, deve existir uma linha telefónica direta e gratuita para o reporte de situações anómalas que esteja operacional a todo momento;

iv. Os talões e informação exibida no ecrã dos ATM e POS da rede são elegíveis;

v. As instituições de apoio assegurem a permanente disponibilidade de dinheiro nos ATM;

vi. Existe um sistema de reserva de energia em todos os locais onde estejam instalados ATM, de modo a garantir que, na sequência de uma falha elétrica da fonte principal, o terminal não interrompa a operação no decorrer de uma transação;

vii. A informação contida no talão ou visível no monitor do terminal não contenha dados que possam facilitar ações de fraude, nomeadamente a clonagem de cartões, caso acontecer o utilizador abandonar o local enquanto uma transação é exibida no monitor, ou esquecer-se de recolher o talão;

viii. Os utilizadores do serviço da rede sejam avisados, através de mensagem visível no ecrã dos ATM ou por outro meio a acordar com as instituições de apoio, com uma antecedência máxima de 48 (quarenta e oito) horas antes de se levar a cabo ações planeadas de manutenção ou interrupção do serviço;

ix. Os ATM da rede são inspecionados periodicamente para monitorização e reporte de atividades e/ou objetos suspeitos;

x. Todos os ATM e POS da rede utilizam sistemas de *software* que são mantidos atualizados contra ameaças de segurança e ataques cibernéticos;

xi. Os aceitantes conhecem as regras para uma correta e segura aceitação do cartão e utilização dos POS da rede, incluindo informações sobre as operações que podem ser realizadas, a identificação dos cartões e dos respetivos titulares e princípios de operação e segurança.

2. Cabe à instituição de apoio:

a) Indicar os supervisores responsáveis pela monitorização e gestão operacional dos seus ATM;

b) Alertar ao operador da rede da ocorrência de qualquer anomalia no funcionamento de ATM;

c) Verificar se os cartões que se encontram no depósito de cartões capturados correspondem aos da listagem obtida, caso contrário deve informar ao operador da rede;

d) Garantir a permanente disponibilidade de dinheiro nos ATM, devendo para tal manter na agência um *stock* de numerário não inferior ao mínimo aconselhado pelo operador da rede para o funcionamento de cada ATM;

e) Contar rigorosamente as notas carregadas em cada cacifo e introduzir o seu valor no *item* correspondente da operação "carregamento";

f) Retirar, e substituir por outros devidamente carregados, os cacifos que transitam do período anterior, caso estes tenham chegado a fornecer notas;

g) Comunicar ao operador da rede, para análise de movimentos de detalhe do período, a incorreção de um fecho contabilístico local;

h) Disponibilizar ao comerciante informação sobre a conta de pagamento associado ao POS, para acolher os movimentos da compensação da rede e as operações de débito e crédito sobre a conta do comerciante decorrentes de fecho do POS, da taxa administrativa de adesão, da faturação mensal, da taxa de instalação de POS e das regularizações.

Artigo 9.º

Dever de informação

1. As instituições financeiras estão obrigadas a informar previamente ao cliente do serviço de uma determinada rede das operações que estão sujeitas à cobrança de taxas, e que taxas serão cobradas (montante e forma como será feita) pelas operações eletrónicas realizadas.

2. As instituições financeiras devem disponibilizar aos utilizadores informações sobre as operações que não se efetuem automaticamente, tais como as transferências eletrónicas, indicando, para tal, o prazo a aguardar até a materialização da operação no sistema.

3. Deve-se optar por uma nomenclatura que possibilite, clara e inequivocamente, a identificação das operações realizadas, destacando-se o valor, data e local, em especial nas situações de informativos de movimentação de conta de qualquer natureza processados por via eletrónica.

4. Aquando da disponibilização de novas operações ou integração de serviços prestados no sistema do serviço da rede, o seu operador deve:

a) Com uma antecedência máxima de 60 (sessenta) dias, comunicar ao Banco de Cabo Verde da sua pretensão e dar-lhe conhecimento de todos os procedimentos a serem realizados;

b) Com uma antecedência máxima de 30 (trinta) dias, disponibilizar aos utilizadores todas as informações necessárias para a sua familiarização com o novo contexto do sistema.

5. Devem os PSP garantir uma maior transparência nas relações contratuais, preservando os utilizadores do serviço, mediante prévio e integral conhecimento das cláusulas contratuais, destacando-se inclusive os dispositivos que imputam responsabilidades, tais como anuidade devida pela prestação do serviço, taxas a serem cobradas sobre a realização das operações eletrónicas e as penalidades.

6. Devem os PSP ou o operador de rede, consoante o caso, num período máximo de 5 (cinco) dias úteis apresentar resposta às consultas, reclamações e pedidos de informação formulados pelos utilizadores, a fim de esclarecer, com brevidade e eficiência, as dúvidas relativas aos serviços prestados no âmbito dessa rede partilhada de pagamentos e processamento de operações financeiras.

7. Devem os PSP garantir que os utilizadores de uma rede têm acesso a toda a informação útil em local e formato visíveis que garantam pleno conhecimento sobre as situações que possam gerar constrangimentos aquando da utilização dos cartões de pagamento na rede, bem como indicar a quem e onde recorrer nesses casos.

8. Devem ser disponibilizados aos utilizadores o endereço, contacto e horário de funcionamento do centro de atendimento, acompanhados da observação de que este se destina ao atendimento, denúncias e reclamações.

Artigo 10.º

Dever de atendimento

O operador, os emitentes e as instituições de apoio que integram uma rede, devem, respetivamente, assegurar e divulgar um serviço de atendimento gratuito, em língua portuguesa, que permita ao utilizador dos serviços da rede, sempre que necessário, estabelecer contacto 24 (vinte e quatro) horas por dia, através de telefone, podendo a instituição, complementarmente a este meio, utilizar um outro indicado nos seus principais canais de difusão de informação.

Artigo 11.º

Dever de sigilo

1. A informação de uma rede é exclusiva e confidencial, e pertence ao respetivo operador.

2. As instituições participantes numa rede devem:

a) Manter as informações confidenciais da rede em estrito secreto;

b) Não divulgar informação confidencial a entidades ou pessoas que não participem no sistema;

c) Conservar e tratar as informações confidenciais, evitando a sua divulgação não autorizada;

d) Divulgar a informação confidencial da rede apenas para os funcionários com necessidade específica de ter dita informação;

e) Fornecer ao Banco de Cabo Verde as informações que este considere necessárias à verificação do seu grau de solvabilidade ou liquidez, do cumprimento das restantes normas legais e regulamentares que disciplinam a sua atividade, da sua organização administrativa e da eficácia dos seus controlos internos.

3. Todo o participante deve tomar medidas adequadas para assegurar que os seus colaboradores ou seus agentes com acesso à rede estejam a par:

a) Da natureza exclusiva e confidencial dos sistemas;

b) Da proibição de dar acesso aos sistemas ou divulgar informação sobre os mesmos a terceiros;

c) Da proibição de utilizar os sistemas para outros fins que não os autorizados nos manuais da rede.

Artigo 12.º

Transações fraudulentas

1. Da responsabilidade do PSP (emitente de cartão ou prestador de serviço através de dispositivo semelhante e/ou instituição de apoio):

a) Quando a fraude tiver como base a adulteração da informação registada nos ATM sob responsabilidade do PSP;

b) Quando a fraude tiver como pressuposto a conivência de pessoal do PSP;

c) Quando a fraude resultar de acasalamento de instrumentos de pagamento e PIN à guarda do PSP;

d) Quando a fraude for provocada por conhecimento das chaves criptográficas da responsabilidade ou à guarda do PSP.

2. Da responsabilidade do operador de rede:

a) Quando forem realizadas transações com instrumentos de pagamento em lista negra, a partir do momento da receção eletrónica da informação ou 24 (vinte e quatro) horas depois da informação por escrito (FAX);

b) Quando a fraude for resultado do desrespeito das normas de segurança internas do operador.

3. Da responsabilidade do comerciante

a) Quando a transação for realizada com um cartão falsificado, sem que todos os dados necessários para o efeito de autorização estejam presentes no pedido ou tenham sido alterados no ponto de atendimento devido a falhas ou não observância dos procedimentos de aceitação;

b) Quando o comerciante realiza uma transação sem o consentimento do consumidor de bens ou serviços, quer seja sem introdução do PIN ou utilizando o CVV2;

c) Quando o utilizador do serviço de pagamento ou titular do cartão ou dispositivo semelhante não participa ou autoriza a transação em ambiente de cartão/dispositivo semelhante não presente, como por exemplo na realização de compras online.

Artigo 13.º

Arquivo de registo de operações e comunicações

As instituições financeiras devem arquivar e conservar, em suporte eletrónico duradouro que permite a sua rastreabilidade, o registo de todas as operações, notificações e demais comunicações efetuadas ao abrigo do presente Aviso, pelo período de 5 anos, contados a partir da data da sua realização.

CAPÍTULO III

ANOMALIAS DE REDE

Secção I

Principais anomalias de uma rede

Artigo 14.º

Incidente com cartão ou dispositivo semelhante

1. Considera-se incidente com cartão ou dispositivo semelhante todo o tipo de incidente em que o utilizador, ainda que por razões alheias à sua vontade e em prejuízo ou beneficio de outrem, resulta beneficiado ou prejudicado numa operação de movimentação de fundos nos terminais de acesso a uma rede.

2. Tipos de operações de movimentação de fundos suscetíveis de originar incidente com cartão ou dispositivo semelhante:

a) Levantamento de numerário;

b) Transferência de fundos para NIB;

c) Pagamento de bens ou serviços;

d) Todo o tipo de serviço disponível em ATM.

3. São incidentes relacionados com levantamentos de numerário, nomeadamente:

a) Disponibilização parcial ou não disponibilização de valor total pelo ATM em uma operação de levantamento;

b) Levantamento diferente do montante solicitado devido a troca de cacifos;

c) Levantamento sem provisão resultante da não atualização do saldo da conta do cliente do PSP na rede.

4. Ocorre um incidente de transferência de fundos para NIB sempre que, na sequência de lapso cometido pelo ordenante da operação na indicação do NIB, os fundos são posteriormente creditados na conta de um outro beneficiário que não o pretendido.

5. São incidentes relacionados com pagamento de bens e serviços, nomeadamente:

a) Não pagamento de bem ou serviço recebido (em detrimento do fornecedor de tais bens e serviços);

b) Débitos sucessivos de igual montante que penalizam o consumidor de bens ou serviços.

6. São incidentes inerentes a todo o tipo de serviço disponível em ATM, nomeadamente:

a) Captura de cartão de pagamento por avaria do ATM, isto é, sem que o cartão esteja expirado ou incluído na lista negra, ou que o utilizador tenha excedido as tentativas de PIN;

b) ATM indica ao utilizador que deve recolher o cartão, mas este não lhe é apresentado para recolha.

Artigo 15.º

Incidente de emitente

Considera-se incidente de emitente toda e qualquer situação em que o emitente deixa de cumprir as suas obrigações, tal como definido no manual de funcionamento do operador de rede, escusando-se de enviar os ficheiros de atualização das contas de clientes ao operador, o que leva a desigualdades de saldos e, consequentemente, a eventuais levantamentos sem provisão.

Artigo 16.º

Incidente de supervisão de terminal de acesso à rede

1. Considera-se incidente de supervisão de ATM toda e qualquer situação resultante de operações de supervisão dos ATM que põem em causa o normal funcionamento do serviço da rede.

2. Incluem-se nesta categoria os seguintes incidentes:

a) Troca de notas nos cacifos;

b) Não comunicação ao operador de rede das sobras de notas;

c) ATM com a indicação de indisponibilidade de dinheiro por tempo superior a 24 (vinte e quatro) horas, incluindo os dias de fins-de-semana e feriados;

d) Indisponibilidade de ATM e/ou POS por tempo superior a 1 (uma) hora, por razões técnicas outras que não se devem à intervenção temporária de manutenção do terminal ou atualização do sistema.

Secção II

Comunicação e circuitos de procedimentos para resolução de anomalias

Artigo 17.º

Comunicação de incidente com cartão ou dispositivo semelhante

1. Disponibilização parcial ou não disponibilização de valor total pelo ATM em uma operação de levantamento:

a) O utilizador que detete ter sido lesado deve comunicar o sucedido ao PSP emitente do respetivo cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante que, pelo seu turno, avisa ao operador de rede do ocorrido;

b) Se, ao analisar a situação, o operador de rede verificar que o montante em falta ficou retido no terminal, deve imediatamente solicitar à instituição de apoio que credite esse montante na conta do utilizador lesado, no prazo máximo de 5 (cinco) dias úteis;

c) Caso contrário, não se verificando a situação anterior, se o operador de rede detetar a existência de um outro utilizador beneficiado:

i. Deve o operador comunicar a ocorrência ao PSP emitente do cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante ao utilizador beneficiado;

ii. O PSP emitente do cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante ao utilizador beneficiado, pelo seu turno, deve notificá-lo para que proceda à regularização da situação dentro dos prazos previstos no n.º 1 do Artigo 20.º deste Aviso, sob pena de ser incluído na lista negra de utilizadores de cartão ou dispositivo semelhante;

iii. Havendo incumprimento das disposições previstas no número anterior, o PSP emitente do cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante deve comunicar o facto ao Banco de Cabo Verde que, pelo seu turno, ordena ao operador de rede o bloqueio de todos e quaisquer cartões ou dispositivo semelhante em nome do utilizador.

2. Levantamento de montante inferior ao solicitado devido a troca de cacifos:

a) O utilizador que detete ter sido lesado deve comunicar o sucedido ao PSP emitente do respetivo cartão ou responsável pela prestação de serviços de pagamento acessíveis através do seu dispositivo semelhante que, pelo seu turno, avisa ao operador de rede do ocorrido;

b) Na sequência, deve o operador de rede solicitar à instituição de apoio que credite o montante em falta na conta do utilizador lesado, no prazo máximo de 5 (cinco) dias úteis.

3. Levantamento de montante superior ao solicitado devido a troca de cacifos:

a) Deve a instituição de apoio, aquando da deteção do incidente, informar ao operador de rede do sucedido;

b) O operador de rede, após analisar a situação, deve informar à instituição de apoio os dados do utilizador envolvido no incidente, devendo igualmente fazer chegar essa informação ao PSP emitente do cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante e ao Banco de Cabo Verde;

c) Por sua vez, deve o PSP emitente do cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante notificar o seu cliente da ocorrência, cabendo a este último regularizar a situação dentro dos prazos previstos no n.º 1 do Artigo 20.º deste Aviso, sob pena de ser incluído na lista negra de utilizadores de cartão ou dispositivo semelhante;

d) Havendo incumprimento das disposições previstas no número anterior, o PSP emitente do cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante deve comunicar o facto ao Banco de Cabo Verde que, pelo seu turno, ordena ao operador de rede o bloqueio de todos e quaisquer cartões ou dispositivo semelhante em nome do utilizador.

4. Levantamento sem provisão na conta:

a) Deve o PSP emitente de cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante, sempre que detete um incidente, notificar o respetivo cliente do sucedido, devendo este último proceder à regularização da situação observando os prazos previstos no n.º 1 do Artigo 20.º deste Aviso, sob pena de ser incluído na lista negra de utilizadores de cartão ou dispositivo semelhante;

b) Havendo incumprimento das disposições previstas no número anterior, o PSP emitente deve comunicar o facto ao Banco de Cabo Verde que, pelo seu turno, ordena ao operador de rede o bloqueio de todos e quaisquer cartões ou dispositivo semelhante em nome do utilizador.

5. Transferência de fundos para NIB erroneamente executadas:

a) Deve o ordenante, aquando da deteção do incidente, no prazo máximo de 2 (dois) dias úteis, entrar em contacto com o respetivo PSP emitente de cartão ou responsável pela prestação de serviços de pagamento através de dispositivo semelhante que, pelo seu turno, comunica ao operador de rede o sucedido;

b) O operador de rede, após analisar a situação, deve reportar a ocorrência ao PSP do destinatário ou cliente beneficiado;

c) O PSP do destinatário ou cliente beneficiado deve notifica-lo da ocorrência, devendo este último regularizar a situação dentro dos prazos previstos no n.º 1 do Artigo 20.º deste Aviso, sob pena de ser incluído na lista negra de utilizadores de cartão ou dispositivo semelhante;

d) Havendo incumprimento das disposições previstas no número anterior, o PSP do destinatário ou cliente beneficiado deve comunicar o facto ao Banco de Cabo Verde que, pelo seu turno, ordena ao operador de rede o bloqueio de todos e quaisquer cartões ou dispositivo semelhante em nome do utilizador.

6. Não pagamento de bem ou serviço recebido:

a) Deve o fornecedor de bens ou serviços, aquando da deteção do incidente, comunicar a ocorrência ao seu PSP e este último inteirar o operador de rede da ocorrência;

b) O operador de rede, após analisar a situação, deve reportar a ocorrência ao PSP do utilizador beneficiado (o comprador);

c) O PSP do utilizador beneficiado deve notificá-lo da ocorrência, devendo este último regularizar a situação dentro dos prazos previstos no n.º 1 do Artigo 20.º deste Aviso, sob pena de ser incluído na lista negra de utilizadores de cartão ou dispositivo semelhante;

d) Havendo incumprimento das disposições previstas no número anterior, o PSP do utilizador beneficiado deve comunicar o facto ao Banco de Cabo Verde que, pelo seu turno, ordena ao operador de rede o bloqueio de todos e quaisquer cartões ou dispositivo semelhante em nome do utilizador.

7. Débitos sucessivos de igual montante que penalizam o consumidor de bens ou serviços:

a) Deve o consumidor de bens ou serviços, aquando da deteção do incidente, comunicar a ocorrência ao seu PSP e este último inteirar o operador de rede da ocorrência;

b) O operador de rede, após analisar a situação, deve reportar a ocorrência à instituição de apoio do fornecedor de bens ou serviços;

c) A instituição de apoio do fornecedor de bens ou serviços deve notificá-lo da ocorrência, devendo este último regularizar a situação dentro dos prazos previstos no n.º 1 do Artigo 20.º deste Aviso, sob pena de lhe ser descontinuado o serviço de POS;

d) Havendo incumprimento das disposições previstas no número anterior, a instituição de apoio do fornecedor de bens ou serviços deve comunicar o facto ao operador de rede;

e) É da obrigação do operador de rede, quando comunicado, mandar suspender o serviço de POS até que o seu cliente regularize o incidente.

8. Captura de cartão de pagamento por avaria do ATM, isto é, sem que o cartão esteja expirado ou incluído na lista negra, ou que o utilizador tenha excedido as tentativas de PIN:

a) O utilizador deve dirigir-se imediatamente ao balcão mais próximo do seu PSP para a resolução do problema;

b) Ao tomar conhecimento da ocorrência, deve o PSP imediatamente entrar em contacto com a instituição de apoio responsável pelo ATM onde se encontra retido o cartão;

c) A instituição de apoio informa o(s) seu(s) supervisor(es) do sucedido e, assim que o cartão dar entrada num dos seus balcões, deve remetê-lo, no prazo máximo de 2 (dois) dias úteis, para o respetivo PSP emitente;

d) Deve o PSP emitente, logo assim que receber o cartão, notificar o seu cliente para efetuar o levantamento do cartão no balcão no qual tem domiciliada a sua conta ou noutro por ele previamente indicado;

e) Nas situações em que o PSP emitente do cartão é também instituição de apoio responsável pelo ATM onde se encontra retido o cartão, aplicam-se os procedimentos que a própria instituição estabelecer.

9. ATM indica ao utilizador que deve recolher o cartão, mas este não lhe é apresentado para recolha:

a) Deve o utilizador aguardar entre 2 (dois) a 3 (três) minutos e, caso persistir a anomalia, informar imediatamente o PSP emitente do cartão ou o operador de rede, através dos contactos do centro de atendimento indicados;

b) Ademais, aplicam-se as mesmas regras previstas no número 8 deste artigo.

Artigo 18.º

Comunicação de incidente de emitente

1. Deve o operador de rede, assim que ficar a par da ocorrência deste tipo de incidente, alertar o PSP emitente para a necessidade de cumprir com as obrigações recomendadas no seu manual de funcionamento, devendo igualmente reportar o facto ao Banco de Cabo Verde.

2. O Banco de Cabo Verde reserva-se, ao abrigo da sua Lei Orgânica, o direito de definir e aplicar penalizações administrativas resultantes do incumprimento sistemático das regras estabelecidas.

Artigo 19.º

Comunicação de incidente de supervisão de terminal de acesso à rede

1. Deve a instituição de apoio comunicar, simultaneamente, ao operador de rede e ao Banco de Cabo Verde, todo e qualquer tipo de incidente de supervisão, até o primeiro dia útil seguinte à sua ocorrência.

2. O Banco de Cabo Verde reserva-se, ao abrigo da sua Lei Orgânica, o direito de definir e aplicar penalizações administrativas resultantes do incumprimento sistemático das regras estabelecidas.

Secção III

Prazos de comunicação

Artigo 20.º

Prazos de comunicação

As comunicações previstas nos artigos que integram a Secção II deste Capítulo devem ser reportadas ao Banco de Cabo Verde observando-se os prazos que a seguir se estabelecem para cada tipo de incidente:

1. Incidente com cartão ou dispositivo semelhante:

a) O PSP emitente deve notificar o cliente beneficiado da ocorrência do incidente com cartão ou dispositivo semelhante, por carta registada com aviso de receção ou outro meio acordado entre as partes, no prazo de 5 (cinco) dias úteis, fazendo-lhe saber que a não regularização do incidente no prazo estabelecido acarretará a sua inclusão na lista negra de utilizadores de cartão ou dispositivo semelhante;

b) A partir da data de receção da notificação referida na alínea anterior, o cliente dispõe de um prazo de até 5 (cinco) dias úteis para proceder a regularização da situação;

c) Por sua vez, o operador de rede dispõe de um prazo nunca superior a 1 (um) dia útil para proceder a normalização da situação junto da instituição de apoio;

d) Na sequência, deve a instituição de apoio de imediato encetar diligências para que a conta do cliente lesado seja creditada pelo devido valor e remeter comunicado ao Banco de Cabo Verde, dando-lhe conhecimento da regularização (ou não) do incidente;

e) Findo o prazo previsto na alínea *b*) deste número, e na eventualidade de incumprimento do mesmo, deve o PSP emitente do cartão ou responsável pela prestação de serviços de pagamento acessíveis através de um dispositivo semelhante do cliente beneficiado comunicar ao Banco de Cabo Verde, em conformidade.

2. Incidente de emitente:

Deve o operador de rede reportar de imediato este tipo de incidente ao Banco de Cabo Verde, a partir do momento que ficar a par da sua ocorrência.

3. Incidente de supervisão de terminal de acesso à rede:

Deve o operador de rede reencaminhar ao Banco de Cabo Verde as comunicações das instituições de apoio sobre ocorrência de incidente de supervisão, logo assim que sejam recebidas.

CAPÍTULO IV

LISTA NEGRA DE UTILIZADORES DE CARTÃO OU DISPOSITIVO SEMELHANTE E CENTRALALIZAÇÃO DE INCIDENTES DE INSTRUMENTOS DE PAGAMENTO

Secção I

Lista Negra de utilizadores de cartão ou dispositivo semelhante

Artigo 21.º

Comunicações ao Banco de Cabo Verde

Não tendo o cliente regularizado a operação no prazo estabelecido na alínea *b*) do n.º 1 do Artigo 20.º, deve o PSP emitente do cartão ou responsável pela prestação de serviços de pagamento acessíveis através de dispositivo semelhante comunicar o sucedido ao Banco de Cabo Verde, no prazo de 5 (cinco) dias úteis.

Artigo 22.º

Comunicações ao operador de rede

Deve o Banco de Cabo Verde comunicar ao operador de rede os dados dos utilizadores que têm processos em regularização, ordenando a sua inclusão numa lista de utilizadores inibidos de usar cartão de pagamento ou dispositivo semelhante, designada lista negra.

Artigo 23.º

Lista negra

1. Deve o operador de rede proceder à inclusão do utilizador na sua lista negra, interditando o uso de cartão ou dispositivo semelhante em qualquer serviço da rede e comunicar, logo de seguida, a informação ao Banco de Cabo Verde.

2. Deve o operador de rede manter um ficheiro histórico com os últimos 6 (seis) meses de movimentos de lista negra comunicados, para efeitos de prova.

Secção II

Incidentes de Pagamento

Artigo 24.º

Gestão e centralização de incidentes

1. Cabe ao Banco de Cabo Verde a gestão e centralização dos incidentes com cartões de pagamento ou dispositivo semelhante, cuja ocorrência coloca em causa o bom funcionamento do Sistema de Pagamentos Cabo-verdiano e tendo em vista o desincentivo do mau uso deste tipo de instrumento.

2. A gestão e centralização da informação de incidentes de pagamento compreende a compilação de toda a informação numa base de dados, para acompanhamento da evolução dos incidentes e identificação de possíveis mecanismos de intervenção no sentido de colmatar tais incidentes.

3. A centralização da informação de incidentes compreende ainda a existência de uma listagem de incidentes de pagamento, constituída pelos utilizadores de cartão de pagamento ou dispositivo semelhante que apresentam risco em termos de utilização deste instrumento de pagamento.

4. A remoção de utilizadores da listagem de incidentes de pagamento é da exclusiva competência do Banco de Cabo Verde, cumpridas as exigências de regularização da operação, acontecendo nunca em um prazo inferior a 60 (sessenta) dias corridos.

5. A divulgação da lista de utilizadores de risco acompanhado dos motivos da sua inclusão é da exclusiva competência do Banco de Cabo Verde e será feita aos intervenientes.

6. O Banco de Cabo Verde definirá em regulamentação própria demais regras de gestão, centralização e divulgação das informações relativas aos incidentes com instrumentos de pagamento.

Artigo 25.º

Intervenientes

São considerados intervenientes no processo de gestão de incidentes com cartão de pagamento ou dispositivo semelhante, as instituições sujeitas à superintendência do Banco de Cabo Verde:

a) PSP:

i. Emitentes;

ii. Instituições de Apoio.

b) Operadores de rede.

Artigo 26.º

Proibição de emissão de cartões ou prestação de serviços de pagamento através de dispositivo semelhante

Enquanto gestor e centralizador dos incidentes de instrumentos de pagamento, pode o Banco de Cabo Verde proibir os PSP a emissão de novos cartões ou prestação de serviços de pagamento através de dispositivo semelhante a utilizadores até que estes regularizem de forma definitiva e completa a operação que originou o(s) incidente(s) comunicado(s) ao Banco de Cabo Verde.

Artigo 27.º

Sigilo

São elementos de uso exclusivo do Banco de Cabo Verde e dos intervenientes os elementos informativos da gestão e centralização dos incidentes de pagamentos, estando vedada a sua utilização fora do âmbito deste e demais regulamentos emitidos pelo Banco de Cabo Verde sobre esta matéria.

CAPÍTULO V

FISCALIZAÇÃO

Artigo 28.º

Competências do Banco de Cabo Verde

Compete ao Banco de Cabo Verde:

1. Através do Departamento de Emissão, Tesouraria e Sistema de Pagamentos – Área de Sistema de Pagamentos – prestar todos os esclarecimentos requeridos sobre o presente Aviso.

2. Adotar as medidas que julgar necessárias, no sentido de garantir o cumprimento pelos destinatários deste Aviso.

3. Proceder à introdução das alterações e regulamentar novas situações que julgar necessárias.

4. Emitir Instruções que venham a ser consideradas necessárias relativamente a orientações específicas para a aplicação operacional do presente Aviso.

5. Deliberar sobre os casos omissos.

CAPÍTULO VI

REGIME SANCIONATÓRIO

Artigo 29.º

Regime aplicável

1. As infrações ao disposto no presente diploma são puníveis nos termos do artigo 31.º do Decreto-legislativo n.º 7/2018, de 28 de novembro, que estabelece o regime jurídico aplicável à regulação, à gestão e ao funcionamento do Sistema de Pagamentos Cabo-verdiano.

2. Aplica-se subsidiariamente o regime geral das contraordenações, aprovado pelo Decreto-legislativo n.º 9/95, de 27 de outubro.

CAPÍTULO VII

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Artigo 30.º

Disposições transitórias

Os operadores de rede partilhada de pagamentos com cartão ou dispositivo semelhante, os PSP emitentes e os PSP que se classificam como instituição de apoio, dispõem de um prazo máximo de 12 (doze) meses para adaptarem a sua organização aos requisitos estabelecidos no artigo 10.º deste Aviso.

Artigo 31.º

Revogação

São revogadas:

a) A Instrução Técnica, anexa à Circular Série A, n.º 123 de 26 de janeiro de 2006.

b) A Instrução Técnica, anexa à Circular Série A, n.º 125 de 06 de novembro de 2006.

Artigo 32.º

Entrada em Vigor

O presente Aviso entra em vigor no dia seguinte ao da sua publicação.

Gabinete do Governador e dos Conselhos do Banco de Cabo Verde, na Praia, aos 10 de junho de 2021. — O Governador, *Óscar Humberto Évora dos Santos.*

Aviso nº 2/2021

Requisitos de segurança para pagamentos efetuados através da *internet*

Na atual conjuntura é comum efetuar-se pagamentos através da *internet* pela comodidade que esse canal proporciona. No entanto, à medida que o uso da *internet* para realizar pagamentos de bens e serviços torna-se usual, questões relacionadas com a segurança dos dados torna-se um fator crítico e fundamental para a aceitação deste tipo de serviço.

A segurança dos pagamentos efetuados através da *internet* constitui uma condição prévia crucial, tanto para os utilizadores como para os prestadores de serviços de pagamento. Os utilizadores são frequentemente alertados sobre incidentes de fraudes, sobretudo relacionados com o acesso aos dados pessoais, e são por isso particularmente sensíveis às questões de segurança em torno dos pagamentos realizados com ou sem cartão através da *internet*.

Com a crescente utilização dos serviços de pagamento através da *internet*, a proteção dos dados pessoais tem-se revelado uma constante preocupação, uma vez que os pagamentos realizados através deste canal implicam, de alguma forma, o processamento de dados pessoais e a utilização de redes de comunicação eletrónicas. De facto, se se pretende que os utilizadores beneficiem plenamente das vantagens dos pagamentos à distância torna-se primordial que os prestadores de serviços de pagamento garantam que as informações sejam mantidas dentro de uma infraestrutura segura com mecanismos de autenticação e de limitação de acesso de terceiros às operações de pagamento, de modo a assegurar a efetiva proteção dos dados.

Em Cabo Verde, o Decreto-legislativo nº 7/2018, de 28 de novembro, veio regular, entre outras matérias relativas ao funcionamento do Sistema de Pagamentos Cabo-verdiano, aspetos relacionados com as regras que os operadores dos sistemas devem estabelecer, para que seja segura a execução de operações de pagamento, onde se incluem operações realizadas através da *internet*. De acordo com o referido diploma, os sistemas devem possuir regras escritas, concernentes à sua administração, gestão e operação, cabendo ao Banco de Cabo Verde também a emissão de instruções nestes domínios.

É nesta ótica, que o Banco de Cabo Verde sublinha a importância de os prestadores de serviços reforçarem a segurança dos pagamentos efetuados através da *internet*, com vista a fortalecer a prevenção e o combate à fraude, e por essa via, a confiança do público.

E neste sentido, ao abrigo do n.º 4 do artigo 17º do Decreto-Legislativo nº 7/2018, de 28 de novembro, o BCV determina o seguinte:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1º

Objeto

1. O presente Aviso estabelece os requisitos mínimos e os conteúdos essenciais aplicáveis à segurança na execução de operações de pagamentos efetuados através de *internet*.

2. O disposto no presente Aviso não invalida a responsabilidade dos Prestadores de Serviços de Pagamento em matéria de controlo e de avaliação dos riscos, de desenvolvimento das suas próprias políticas de segurança e de implementação de medidas adequadas de segurança, de contingência, de gestão de incidentes e de continuidade do negócio proporcionais aos riscos inerentes aos serviços de pagamento prestados.

Artigo 2º

Âmbito

1. O presente Aviso aplica-se à prestação de serviços de pagamento, descritos no artigo 2º, do Decreto-legislativo nº 8/2018, disponibilizados através da *internet* pelos PSP.

2. Os requisitos mínimos referidos no número 1 do artigo 1º aplicam-se aos pagamentos feitos através da *internet*, numa das seguintes formas:

a) Cartão – execução de operações de pagamento com cartão à distância através de *internet*, incluindo pagamentos com cartão virtual;

b) Transferência a crédito – realização de transferências a crédito via *internet* através de um portal bancário;

c) Débitos diretos - emissão e alteração de autorização eletrónica de débitos;

d) Moeda eletrónica – execução de transferência de moeda eletrónica entre duas contas de pagamento através de *internet*;

e) Outras que possam vir a ser utilizadas.

3. Ficam excluídos do âmbito de aplicação do presente Aviso as seguintes operações:

a) Outros serviços de *internet* prestados por um PSP através do seu sítio web de pagamento;

b) Pagamentos em que a instrução é comunicada através de correio, por telefone, correio de voz ou utilizando tecnologia baseada em SMS (*Short Message Service)*;

c) Pagamentos móveis, exceto pagamentos baseados em navegadores (*browsers*);

d) Transferências a crédito em que terceiros têm acesso à conta de pagamento do utilizador de serviços de pagamento;

e) Operações de pagamento efetuadas por uma empresa através de redes dedicadas;

f) Pagamentos com cartão, utilizando cartões pré-pagos físicos ou virtuais anónimos e não recarregáveis em que não existe uma relação contínua entre o emitente e o titular do cartão;

g) Compensação e liquidação de operações de pagamento.

Artigo 3º

Definições

Para efeitos do presente diploma, consideram-se as seguintes definições:

a) «Autenticação» *é* o procedimento que permite ao PSP verificar a identidade de um utilizador de serviços de pagamento;

b) «Autenticação forte do utilizador do serviço de pagamento» é o procedimento baseado na utilização de dois ou mais dos seguintes elementos – classificados como conhecimento, posse e inerência:

i) algo que apenas o utilizador conhece, por exemplo uma palavra-passe estática, um código, um número de identificação pessoal;

ii) algo que apenas o utilizador possui, designadamente, um dispositivo de autenticação (*token*), um cartão inteligente, um telemóvel;

iii) alguma característica inerente ao utilizador, nomeadamente uma característica biométrica.

c) «Autorização» é um procedimento que verifica se um utilizador de serviços de pagamento ou um PSP tem o direito de executar uma determinada ação, por exemplo o direito de transferir fundos ou de ter acesso a dados sensíveis;

d) «Credenciais» são as informações, geralmente confidenciais, fornecidas por um utilizador de serviços de pagamento ou por um PSP, para efeitos de autenticação. As credenciais podem também dizer respeito à posse de um instrumento físico que contém informações (por exemplo, um gerador de palavras-passe de uso único, um cartão inteligente) ou alguma coisa que o utilizador memoriza ou representa (tais como características biométricas);

e) «Incidente de segurança dos pagamentos de caráter severo» é um incidente que tem ou poderá ter um impacto material sobre a segurança, a integridade ou a continuidade dos sistemas relacionados com pagamentos do PSP e/ou a segurança de dados de pagamento sensíveis ou de fundos;

f) «Análise de risco da operação» é a avaliação do risco associado a uma operação específica, tendo em conta critérios como os padrões de pagamento do utilizador de serviços de pagamento (comportamento), o valor da operação relacionada, o tipo de produto e o perfil do beneficiário;

g) «Cartão virtual» é uma solução de pagamento baseada num cartão cujo número é temporário e alternativo, com um período de validade reduzido, uma utilização limitada e um limite de despesa predefinido, que pode ser utilizado para efetuar compras através da *internet;*

h) «Carteira virtual» é a solução que permite a um utilizador de serviços de pagamento registar dados relacionados com um ou mais instrumentos de pagamento, a fim de realizar pagamentos com várias entidades de comércio eletrónico;

i) «Encriptação ponto-a-ponto» refere-se à encriptação na origem da comunicação, enquanto a desencriptação correspondente ocorre no recetor final;

j) «IP (*Internet Protocol*)» é um código numérico exclusivo que identifica cada computador ligado a *internet;*

k) «Palavra passe de uso único (*One Time Password - OTP*)» consiste numa senha que é válida somente para realizar uma única operação de pagamento, evitando, assim, que alguém que a intercete, a possa utilizar novamente com sucesso;

l) «Princípio da minimização de dados» refere-se à política de recolha do mínimo de informação pessoal necessária para executar uma determinada função;

m) «Princípio do privilégio mínimo» é o princípio que define que os operadores devem ter os privilégios mínimos e necessários para completar uma tarefa de modo que ocorrendo alguma falha este tenha o mínimo impacto possível.

CAPÍTULO II

AMBIENTE GERAL DE CONTROLO E DE SEGURANÇA

Artigo 4º

Política de segurança

Tendo em conta o disposto na alínea *d*) do número 1, do artigo 10º, do Decreto-legislativo nº 7/2018 e a correspondente regulamentação dos requisitos mínimos, os PSP devem implementar uma política de segurança formal para os serviços de pagamentos prestados através da *internet*.

Artigo 5º

Quadro de avaliação global dos riscos

1. Em conformidade com a alínea *c*), do nº 1, do artigo10º, do Decreto-legislativo nº7/2018, de 28 de novembro, qualquer sistema de prestação de serviços de pagamento através da *internet* deve dispor de mecanismos de gestão de riscos adequados à gestão, controlo e comunicação dos riscos a que estejam ou possam vir a estar expostos.

2. Os PSP devem implementar um quadro de avaliação dos riscos, com instrumentos de gestão de riscos sólidos e adequados ao nível de risco identificado, que lhes permita aferir o risco subjacente aos serviços de pagamento através da *internet* que pretendem implementar assim como monitorizar os riscos após a sua entrada em funcionamento.

3. O processo de avaliação dos riscos deve incidir sobre a segurança dos pagamentos efetuados através da *internet*, os procedimentos e os serviços relacionados, o ambiente tecnológico, a proteção e segurança dos dados sensíveis dos pagamentos e, ainda, sobre os cenários de riscos e mecanismos de segurança observados após a ocorrência de incidentes graves.

4. Os resultados das avaliações de riscos efetuados devem ser submetidos à aprovação pela administração, responsável pelo sistema de avaliação e controlo dos riscos.

5. A revisão do quadro geral de avaliação dos riscos deve ser feita anualmente.

Artigo 6º

Monitorização e procedimentos de reporte de incidentes

1. Os PSP têm as seguintes responsabilidades no âmbito da monitorização e gestão dos incidentes:

a) Assegurar a monitorização, o tratamento e o acompanhamento dos incidentes de segurança, incluindo as reclamações de utilizadores de serviços de pagamento;

b) Adotar procedimentos de reporte desses incidentes aos órgãos de administração e fiscalização e, em caso de incidentes de segurança dos pagamentos de carácter severo às autoridades de supervisão;

c) Tratar e acompanhar os incidentes de segurança e as reclamações de utilizadores de serviços de pagamento relacionadas com a segurança e reportar os mesmos à administração e nos casos de incidentes mais graves instituir procedimentos visando informar imediatamente as autoridades de supervisão e de proteção de dados;

d) Adotar procedimentos de cooperação com as autoridades responsáveis pela aplicação da lei relevante nas situações de incidentes de segurança dos pagamentos de caráter severo incluindo violações de dados;

2. Os procedimentos descritos no número 1 do presente artigo aplicam-se, igualmente, às entidades contratadas pelos PSP para prestação dos seus serviços, devendo estes últimos exigir contratualmente que aqueles cumpram com os referidos procedimentos.

3. Caso a entidade subcontratada não coopere com as autoridades, o PSP deve tomar medidas para fazer cumprir a obrigação contratual ou resolver o contrato sob pena de ser responsabilizado pela entidade reguladora.

Artigo 7º

Controlo e mitigação de riscos

Os PSP obrigam-se a implementar medidas para mitigar os riscos detetados de acordo com a sua política de segurança, devendo para tal:

a) Garantir a separação adequada de funções em ambientes de tecnologias de informação (TI) e a implementação adequada do princípio do "privilégio mínimo", em todas as etapas de implementação dos serviços de pagamentos através de *internet*;

b) Dispor de soluções de segurança adequadas para proteger as redes, os *web site*, os servidores e as hiperligações de comunicação contra violações ou ataques, devendo desativar todas as funções desnecessárias dos servidores, de modo a protegê-los e a eliminar ou a reduzir as vulnerabilidades de aplicações em risco;

c) Limitar, ao mínimo, o acesso de várias aplicações aos dados e aos recursos exigidos, de acordo com o princípio do "privilégio mínimo";

d) Garantir que os *web sites* que oferecem serviços de pagamento através da internet sejam identificados por certificados de validação digital criados em nome do PSP ou através de outros métodos de autenticação semelhantes, visando limitar a utilização de *web site* "falsos";

e) Implementar processos adequados para monitorizar, detetar e limitar o acesso a dados sensíveis de pagamentos e recursos lógicos críticos, tais como redes, sistemas, bases de dados, módulos de segurança etc. Os PSP devem, ainda, criar, guardar e analisar os registos e as pistas de auditoria;

f) Certificar que o princípio da minimização de dados seja uma componente essencial da funcionalidade principal, ou seja, a recolha, o encaminhamento, o processamento, o armazenamento e /ou arquivamento e a visualização de dados de pagamento sensíveis devem ser mantidos num nível mínimo absoluto, durante a conceção, o desenvolvimento e a manutenção de serviços de pagamento através da *internet*;

g) Testar sob fiscalização da função de gestão de riscos os mecanismos de segurança para os serviços de pagamento através da *internet*, a fim de garantir a sua solidez e eficácia;

h) Garantir que os mecanismos de segurança para pagamentos de serviços através da *internet* bem como o seu funcionamento sejam auditados regularmente com vista a assegurar a sua consistência e eficácia. A frequência e o foco destas auditorias devem ter em consideração os riscos de segurança envolvidos e devem ser proporcionais aos mesmos. As auditorias devem ser realizadas por especialistas qualificados e independentes (internos ou externos) e que não estejam envolvidos, seja de que forma for, no desenvolvimento, na implementação ou na gestão operacional dos serviços de pagamento prestados através da *internet*;

i) Garantir que os contratos celebrados com entidades que prestam serviços relacionadas com a segurança de serviços de pagamento, para os PSP, incluem disposições que obrigam ao cumprimento dos princípios e das normas estabelecidas neste Aviso;

j) Exigir contratualmente, no caso dos PSP que oferecem serviços de aceitação (*acquiring*), que as entidades de comércio eletrónico que processem dados de pagamento sensíveis implementem medidas de segurança na sua infraestrutura de TI, em conformidade com o estabelecido nas alíneas *a*) e i) do presente artigo, a fim de evitar o roubo dos dados através dos seus sistemas;

k) Tomar as medidas para se fazer cumprir as obrigações contratuais ou resolver o contrato, se tomar conhecimento de que um comerciante eletrónico não implementou as medidas de segurança referidas na alínea anterior.

Artigo 8º

Rastreabilidade

Os PSP obrigam-se a implementar processos que garantam que todas as operações, assim como o fluxo do processo da autorização eletrónica de débito em conta são rastreados adequadamente. Para tal os PSP devem:

a) Assegurar que o seu serviço inclui mecanismos de segurança para o registo detalhado de dados da operação e da autorização eletrónica de débito em conta, do qual deve constar o número sequencial da operação, os carimbos temporais para os dados da operação, as alterações de parametrização, assim como o acesso aos dados da operação e da autorização eletrónica de débito em conta;

b) Implementar ficheiros de registo (*logs*) que permitam rastrear qualquer aditamento, alteração ou exclusão de dados da operação e da autorização eletrónica de débito em conta;

c) Consultar e analisar os dados da operação e da autorização eletrónica de débito em conta e assegurar que possuem meios para avaliar os ficheiros de registo e que as respetivas aplicações estejam acessíveis somente aos colaboradores devidamente autorizados para o efeito e no âmbito do desempenho das suas funções.

CAPÍTULO III

MECANISMOS DE CONTROLO ESPECÍFICOS E MEDIDAS DE SEGURANÇA PARA PAGAMENTOS ATRAVÉS DA *INTERNET*

Artigo 9º

Identificação inicial do utilizador de serviços de pagamento

1. Os utilizadores de serviços de pagamento devem ser devidamente identificados, em conformidade com a legislação cabo-verdiana relativa à prevenção de lavagem de capitais e do financiamento ao terrorismo, e devem confirmar a sua vontade de realizar pagamentos através da *internet*, antes de lhes ser concedido o acesso a esses mesmos serviços.

2. Os PSP devem, antecipadamente, de forma regular ou se necessário *ad hoc*, fornecer informações adequadas ao utilizador de serviços de pagamento, sobre os requisitos necessários para realizar operações de pagamento seguras através da *internet* e sobre os riscos associados.

3. Os PSP devem assegurar que o utilizador de serviços de pagamento foi submetido aos procedimentos de identificação e verificação do utilizador de serviços de pagamento e que forneceu os documentos de identificação exigidos, assim como informações relacionadas, antes de lhe ser concedido o acesso aos serviços de pagamento através da *internet*.

4. Os PSP devem assegurar que a informação prévia fornecida ao utilizador de serviços de pagamento, conforme determinado no regime jurídico dos serviços de pagamentos e de emissão da moeda eletrónica, Decreto-legislativo nº 8/2018, de 28 de novembro, contém toda a informação prevista na legislação e, adicionalmente, os detalhes específicos relacionados com os serviços de pagamento através da *internet*.

5. Os detalhes referidos no número anterior devem incluir, sempre que se considere adequado:

a) Informações claras sobre quaisquer requisitos em termos de equipamento do utilizador de serviços de pagamento, *software* ou outros instrumentos necessários (por exemplo, *software,* antivírus*, firewalls* etc.);

b) Regras para a utilização adequada e segura de credenciais de segurança personalizadas;

c) Descrição passo-a-passo dos procedimentos a observar pelo utilizador de serviços de pagamento para a apresentação e a autorização de uma operação de pagamento e/ou a obtenção de informações, incluindo as consequências de cada ação;

d) Regras para a utilização adequada e segura de todo o *hardware* e *software* fornecidos ao utilizador de serviços de pagamento;

e) Os procedimentos a observar em caso de perda ou de furto das credenciais de segurança personalizadas ou do *hardware* ou do *software* do utilizador de serviços de pagamento para início de sessão ou para execução das operações;

f) Os procedimentos a observar em caso de suspeita ou de deteção de uma utilização abusiva;

g) Descrição das responsabilidades e das obrigações do PSP e do utilizador de serviços de pagamento, respetivamente, no que tange à utilização do serviço de pagamento através da *internet*.

6. Os PSP devem assegurar, sempre que as operações de pagamento sejam abrangidas por um contrato quadro, que o utilizador de serviços de pagamento indique, claramente, a possibilidade do PSP bloquear uma determinada operação ou o instrumento de pagamento por razões de segurança.

7. O PSP deve estabelecer o método e os termos da notificação do utilizador de serviços de pagamento e a forma como o utilizador de serviços de pagamento pode contactar o PSP, para que a operação ou o serviço de pagamento através da *internet* seja "desbloqueado".

Artigo 10º

Autenticação forte do utilizador de serviços de pagamento

1. A iniciação de pagamentos através da *internet*, assim como o acesso aos dados de pagamento sensíveis, deve ser protegida por uma autenticação forte do utilizador de serviços de pagamento.

2. Os PSP devem implementar procedimentos de autenticação forte do utilizador de serviços de pagamento de acordo com a definição estabelecida no presente Aviso.

3. Para as operações baseadas em cartão/autorização eletrónica de débito em conta de pagamento, os PSP devem realizar uma autenticação forte do utilizador de serviços de pagamento para a autorização de operações de pagamento através da *internet* e para a emissão ou a alteração de autorizações eletrónicas de débito direto.

4. Os PSP podem adotar medidas alternativas de autenticação do utilizador de serviços de pagamento para as seguintes situações:

a) Pagamentos efetuados a beneficiários de confiança incluídos em listas positivas estabelecidas previamente para esse utilizador de serviços de pagamento;

b) Operações entre duas contas do mesmo utilizador de serviços de pagamento detidas junto do mesmo PSP;

c) Transferências justificadas por uma análise de risco da operação, nos termos que vierem a ser estabelecidos pelo Banco de Cabo Verde;

d) Operações de pagamento de baixo valor, tal como definido no artigo 27º do Decreto-legislativo nº 8/2018, de 28 de novembro.

5. A obtenção de acesso ou a alteração de dados sensíveis de pagamento exigem uma autenticação forte do utilizador de serviços de pagamento. Nas situações em que o PSP presta serviços meramente consultivos, a exemplo de dados do cartão de pagamento, que podem facilmente ser usados de forma inadequada para praticar fraudes, o PSP pode adaptar os seus requisitos de autenticação com base na sua avaliação de riscos.

6. No caso de operações com cartões, todos os PSP emitentes devem adotar a autenticação forte do titular do cartão e os cartões emitidos devem estar tecnicamente preparados/registados para serem utilizados com a autenticação forte.

7. Os PSP que oferecem serviços de aceitação (*acquiring*) devem adotar tecnologias que permitam que o emitente proceda à autenticação forte do titular do cartão para os sistemas de pagamento com cartão, nos quais o adquirente participa.

8. Os PSP que oferecem serviços de aceitação (*acquiring*) devem exigir que a sua entidade de comércio eletrónico adota soluções que possibilitem ao emitente realizar uma autenticação forte do titular do cartão para operações com cartão através da *internet*.

9. Para efeitos do previsto no número anterior, podem ser utilizados métodos de autenticação alternativos para categorias pré-definidas de operações de baixo risco, por exemplo, com base na análise de risco da operação ou no caso de pagamentos de baixo valor, sem prejuízo do determinado pelo Decreto-Legislativo nº8/2018, de 28 de novembro.

10. Para os sistemas de pagamento com cartão aceites pelo serviço, os fornecedores de carteiras virtuais devem exigir uma autenticação forte por parte do emitente, no momento em que o legítimo titular regista os dados do cartão pela primeira vez.

11. Os fornecedores de carteiras virtuais devem suportar a autenticação forte do utilizador de serviços de pagamento, quando estes utilizadores de serviços de pagamento iniciam a sessão nos serviços de pagamento com carteiras ou realizam operações com cartão através da *internet*.

12. No caso de cartões virtuais, o registo inicial deve ser realizado em ambiente seguro e de confiança. Se o cartão for emitido através da *internet*, deve ser exigida a autenticação forte do utilizador de serviços de pagamento para o processo de criação de dados do cartão virtual.

13. Os PSP devem assegurar a autenticação bilateral adequada durante a comunicação com entidades de comércio eletrónico para efeitos de iniciação de pagamentos através da *internet* e de acesso a dados de pagamento sensíveis.

Artigo 11º

Pedido de disponibilização de instrumentos de autenticação e/ou de *software* fornecido ao utilizador de serviços de pagamento

1. Os PSP devem assegurar que o primeiro pedido do utilizador de serviços de pagamento para disponibilização de instrumentos/ferramentas de autenticação necessários para utilizar o serviço de pagamento através da *internet* e/ou o fornecimento aos utilizadores de serviços de pagamento de *software* relacionado com o pagamento são efetuados de forma segura.

2. O pedido e a disponibilização de instrumentos/ferramentas de autenticação e/ou *software* relacionado com o pagamento, fornecido ao utilizador de serviços de pagamento, devem preencher os seguintes requisitos:

a) Os procedimentos relacionados devem ser realizados num ambiente seguro e de confiança, tendo em conta os possíveis riscos decorrentes da utilização de dispositivos/equipamentos que os PSP não controlam;

b) Devem ser implementados procedimentos eficazes e seguros para o fornecimento de credenciais de segurança personalizadas, de *software* relacionado com pagamento e de todos os dispositivos/equipamentos personalizados relacionados com pagamentos através da *internet*;

c) O *software* fornecido através da *internet*, também, deve ser assinado digitalmente pelo PSP, a fim de permitir que o utilizador de serviços de pagamento verifique a sua autenticidade e assegure que este não foi manipulado;

d) Para transações com cartão, o utilizador de serviços de pagamento deve ter a opção de registo para garantir a autenticação forte, independentemente da realização de uma compra específica através da *internet*. Sempre que, durante a realização de compras na *internet*, seja disponibilizada a ativação, este processo deve ser efetuado através do encaminhamento do utilizador de serviços de pagamento para um ambiente seguro e de confiança;

e) Os emitentes de cartões devem encorajar ativamente o titular do cartão a efetuar uma autenticação forte e não devem permitir que os titulares dos cartões ultrapassem essa autenticação senão em casos excecionais e limitados, justificados pelo risco associado a uma determinada transação com cartão.

Artigo 12º

Tentativas de início de sessão, tempo limite de sessão excedido, validade da autenticação

1. Os PSP devem limitar o número de tentativas de início de sessão ou de autenticação, definir regras para o «tempo limite» da sessão de serviços de pagamento através da *internet* e definir limites temporais para a validade da autenticação.

2. Aquando da utilização de uma palavra-passe de uso único, para fins de autenticação, os PSP devem assegurar que o período de validade dessas palavras-passe está limitado ao mínimo necessário.

3. Os PSP devem estabelecer o número máximo de tentativas falhadas de início de sessão ou de autenticação após o qual o acesso ao serviço de pagamento através da *internet* é, temporariamente ou permanentemente, bloqueado.

4. Os PSP devem implementar um procedimento seguro para reativar os serviços de pagamento através da *internet* bloqueados.

5. Os PSP devem estabelecer o período máximo após o qual as sessões inativas dos serviços de pagamento através da *internet* são automaticamente terminadas.

Artigo 13º

Monitorização de operações

1. Os mecanismos de monitorização de operações concebidos para evitar, detetar e bloquear operações de pagamento fraudulentas devem ser executados antes da autorização final do PSP.

2. As operações de risco elevado, ou as suspeitas de tais operações, devem ser sujeitas a um procedimento específico de filtragem e de avaliação.

3. Os PSP devem implementar mecanismos de monitorização de segurança e de autorização equivalentes para a emissão de autorizações eletrónicas de débito em conta.

4. Os PSP devem utilizar sistemas de deteção e de prevenção de fraude para identificar operações suspeitas antes da autorização das operações ou das autorizações eletrónicas de débito em conta.

5. Os sistemas a que o número anterior se refere devem:

a) Basear-se, nomeadamente, em regras parametrizadas (tais como listas negras de dados de cartões comprometidos ou furtados) e devem monitorizar padrões de comportamento anormais do utilizador de serviços de pagamento ou do dispositivo de acesso do utilizador de serviços de pagamento (tais como uma alteração do endereço do Protocolo de *internet* (IP) ou do alcance do IP durante a sessão de serviços de pagamento através da *internet*, por vezes identificada através de verificações de IP por localização geográfica, categorias de entidades de comércio eletrónico atípicas para um determinado utilizador de serviços de pagamento ou dados de operações atípicas, etc.);

b) Conseguir detetar sinais de existência de *software* malicioso na sessão (por exemplo, distinguir a ação de um *script* malicioso de uma ação/validação humana) e de cenários de fraude conhecidos.

6. O grau, a complexidade e a adaptabilidade das soluções de monitorização devem ser consentâneos com o resultado da avaliação de riscos e cumprir a legislação de proteção de dados relevante.

7. Os PSP adquirentes (*acquirers*) devem implementar sistemas de deteção e de prevenção de fraude para monitorizar as atividades das entidades de comércio eletrónico.

8. Os PSP devem realizar quaisquer procedimentos de triagem e de avaliação de operações dentro de um prazo adequado, de modo a não atrasar indevidamente a iniciação e/ou a execução do serviço de pagamento em questão.

9. Sempre que o PSP, de acordo com a sua política de risco, decide bloquear uma operação de pagamento que foi identificada como potencialmente fraudulenta, o PSP deve manter o bloqueio durante o mínimo de tempo possível, até que sejam resolvidos os problemas de segurança.

Artigo 14º

Proteção de dados sensíveis de pagamento

1. Os dados sensíveis de pagamento devem ser protegidos durante o seu armazenamento, tratamento ou transmissão, conforme o disposto no artigo 53º do Decreto-Legislativo nº 8/2018, de 28 de novembro.

2. Todos os dados utilizados para identificar e autenticar os utilizadores de serviços de pagamento (por exemplo, no início de sessão, ao iniciar pagamentos através da *internet* e durante a emissão, a alteração ou o cancelamento de autorizações eletrónicas de débito em conta), e a interface do utilizador de serviços de pagamento (site *web* do PSP ou da entidade de comércio eletrónico), devem ser protegidos de forma adequada contra roubo e acesso ou alteração não autorizada.

3. Os PSP devem assegurar que, durante as transferências de dados de pagamento sensíveis através da *internet*, é utilizada uma encriptação segura ponto-a-ponto (*'secure end-to-end encryption'*) entre as partes que comunicam através da respetiva sessão de comunicação, de forma a salvaguardar a confidencialidade e a integridade dos dados, a qual deve usar técnicas de encriptação fortes e amplamente reconhecidas.

4. Os PSP que oferecem serviços de aceitação (*acquiring*) devem encorajar as entidades de comércio eletrónico por si apoiadas a não armazenar quaisquer dados de pagamento sensíveis.

5. Caso as entidades de comércio eletrónico processem (ou seja, armazenem, tratem ou transmitam) dados sensíveis de pagamento, esses PSP devem exigir contratualmente que as entidades de comércio eletrónico implementem as medidas necessárias para proteger esses dados.

6. Os PSP devem realizar verificações regulares e, caso um PSP tome conhecimento de que uma entidade de comércio eletrónico que trata de dados sensíveis de pagamento não implementou as medidas de segurança exigidas, deverá tomar medidas para fazer cumprir esta obrigação contratual ou resolver o contrato.

CAPÍTULO IV

SENSIBILIZAÇÃO, EDUCAÇÃO E COMUNICAÇÃO COM O UTILIZADOR DE SERVIÇOS DE PAGAMENTO

Artigo 15º

Educação e Comunicação

1. Os PSP devem assistir e orientar os utilizadores de serviços de pagamento, sempre que necessário, no que se refere à utilização segura dos serviços de pagamento através da *internet*.

2. Os PSP devem comunicar com os seus utilizadores de serviços de pagamento de modo a tranquilizá-los sobre a autenticidade das mensagens recebidas.

3. Os PSP devem fornecer, pelo menos, um canal seguro (por exemplo, uma caixa de correio dedicada no seu sítio *web* do PSP ou um sítio *web* seguro) para a comunicação permanente com os utilizadores de serviços de pagamento relativamente à utilização correta e segura do serviço de pagamento através da *internet*.

4. Os PSP devem informar os utilizadores de serviços de pagamento sobre a existência do canal referido no número anterior e explicar que qualquer mensagem em nome do PSP enviada através de quaisquer outros meios, nomeadamente de e-mails, respeitante à utilização correta e segura do serviço de pagamento através da *internet*, não é fiável.

5. O PSP deve, ainda, explicar aos utilizadores de serviços de pagamento:

a) Os procedimentos de reporte que devem ser adotados em caso de suspeitas de pagamentos fraudulentos, incidentes suspeitos ou anomalias durante a utilização de serviços de pagamento através da *internet* e/ou possíveis tentativas de engenharia social, isto é, técnicas de manipulação de pessoas de forma a obter informações, quer seja através de e-mail, de chamadas telefónicas ou, ainda, de recolha de informações em redes sociais para fins de fraudes;

b) Os procedimentos seguintes, ou seja, como é que o PSP responderá ao utilizador de serviços de pagamento e como o notificará sobre (potenciais) operações fraudulentas ou como o avisará sobre a ocorrência de ataques (por exemplo, *e-mails* de *phishing*).

6. Através do canal seguro, os PSP devem manter os utilizadores de serviços de pagamento informados sobre atualizações de procedimentos de segurança relativos a serviços de pagamento através da *internet*.

7. Quaisquer alertas sobre riscos emergentes significativos (como avisos sobre engenharia social) também devem ser disponibilizados através do canal seguro.

8. A assistência ao utilizador de serviços de pagamento deve ser disponibilizada pelos PSP para todas as questões, reclamações, pedidos de apoio e notificações de anomalias ou incidentes relativos a pagamentos através da *internet* e a serviços relacionados e os utilizadores de serviços de pagamento devem ser informados sobre a forma como podem obter essa assistência.

9. Os PSP devem apostar em programas de educação e de sensibilização dos utilizadores de serviços de pagamento de forma a assegurar que estes compreendem, no mínimo, a necessidade de:

a) Protegerem as suas palavras-passe, *tokens* de segurança, informações pessoais e outros dados confidenciais;

b) Gerirem adequadamente a segurança do seu dispositivo pessoal (como o computador), através da instalação e da atualização de componentes de segurança (antivírus, *firewalls*, atualizações de segurança);

c) Considerarem as ameaças e os riscos significativos relacionados com a transferência de *software* através da *internet*, no caso de o utilizador de serviços de pagamento não estar razoavelmente seguro de que o *software* é genuíno e não foi manipulado;

d) Utilizarem o sítio *web* genuíno de pagamento através da *internet* do PSP.

10. Os PSP adquirentes devem exigir que as entidades de comércio eletrónico separem claramente os processos relacionados com pagamentos da loja *online*, de modo a que os utilizadores de serviços de pagamento identifiquem mais facilmente quando estão a comunicar com o PSP e não com o beneficiário (por exemplo, redirecionando o utilizador de serviços de pagamento e abrindo uma janela separada de forma a que o processo de pagamento não seja apresentado numa janela *(frame* da entidade de comércio eletrónico).

Artigo 16º

Notificação ao utilizador de serviços de pagamento e definição de limites

1. Os PSP devem definir limites para os serviços de pagamento através da *internet* e podem oferecer aos seus utilizadores de serviços de pagamento opções para a limitação adicional de riscos dentro destes limites. Os PSP podem também fornecer serviços de alerta e de gestão do perfil do utilizador de serviços de pagamento.

2. Antes da disponibilização ao utilizador de serviços de pagamento através da *internet*, os PSP devem definir limites aplicáveis a esses serviços, (por exemplo, um montante máximo para cada pagamento individual ou um montante cumulativo durante um determinado período de tempo) e devem informar os seus utilizadores de serviços de pagamento em conformidade.

3. Os PSP devem permitir que os utilizadores de serviços de pagamento desativem a funcionalidade de pagamento através da *internet*.

Artigo 17º

Acesso do utilizador de serviços de pagamento a informação sobre o estado da iniciação e da execução do pagamento

1. Os PSP devem confirmar aos seus utilizadores de serviços de pagamento a iniciação do pagamento e devem fornecer, de forma atempada nos termos do Título II, do capítulo 1, do Decreto-legislativo nº 8/2018, de 28 de novembro, a informação necessária para a verificação de que a operação de pagamento foi iniciada e/ou executada corretamente.

2. Para as operações baseadas em cartão/autorização eletrónica de débito em conta, os PSP devem fornecer aos utilizadores de serviços de pagamento, num ambiente seguro e de confiança, um sistema, quase em tempo real, de verificação do estado de execução das operações, assim como, a qualquer momento, os saldos das contas.

3. Quaisquer demonstrações eletrónicas detalhadas devem ser disponibilizadas num ambiente seguro e de confiança. Sempre que os PSP informem os utilizadores de serviços de pagamento sobre a disponibilidade de demonstrações eletrónicas (por exemplo, de forma regular, após a emissão de uma demonstração eletrónica periódica, ou numa base *ad hoc*, após a execução de uma operação) através de um canal alternativo, tal como através de SMS, de *e-mail* ou de carta, os dados de pagamento sensíveis não devem ser incluídos nessas comunicações ou, caso sejam incluídos, devem ser ocultados.

CAPÍTULO V

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Artigo 18º

Disposições transitórias

Os PSP que à data da publicação deste normativo não cumprem com os requisitos definidos devem, no prazo de um ano, a contar da data da sua publicação, criar as condições de modo a observar integralmente as normas estipuladas.

Artigo 19º

Regime supletivo

Em tudo em que não se encontre previsto no presente Aviso é aplicável o Regime Jurídico do Sistema de Pagamentos Cabo-verdiano, regulado pelo Decreto-legislativo n.º 7/2018, de 28 de novembro.

Artigo 20º

Obrigatoriedade de reporte

Os prestadores de serviços de pagamento, referidos no nº 1 do artigo 2º do presente Aviso, onde estão sedeadas as contas de pagamento sobre as quais recaem eventuais suspeitas de fraudes, resultando na movimentação de valores a débito ou a crédito sobre as mesmas, obrigam-se a disponibilizar toda a informação necessária ao Banco de Cabo Verde tão logo seja detetada a suspeita de fraude.

Artigo 21º

Comunicação das informações ao Banco de Cabo Verde

A comunicação das informações referidas no artigo anterior deve ser feita através de canais próprios disponibilizados para este fim.

Artigo 22º

Revisão

O Banco de Cabo Verde procederá à revisão deste normativo no prazo que entender adequado, após avaliar a necessidade de se introduzir alterações ao mesmo.

Artigo 23º

Instruções Técnicas

O Banco de Cabo Verde pode emitir instruções que venham a ser consideradas necessárias relativamente a orientações específicas para a aplicação operacional do presente Aviso.

Artigo 24º

Entrada em vigor

Este Aviso entra em vigor no dia seguinte ao da sua publicação.

Gabinete do Governador e dos Conselhos do Banco de Cabo Verde, na Praia, aos 10 de junho de 2021. — O Governador, *Óscar Humberto Évora dos Santos*.

Aviso nº 3/2021

Requisitos de segurança para pagamentos efetuados através de dispositivos móveis

A globalização das economias, aliada ao avanço de novas tecnologias, com produtos digitais que permitem a conexão das pessoas numa base de 24 horas/7 dias em todo mundo, propiciaram inovações nas soluções de pagamento, estabelecendo alternativas para os pagamentos em numerário, cheques e cartões, por outras tecnologias, que são em si, fáceis, rápidas e cómodas, como é o caso dos sistemas de pagamentos que oferecem serviços através de dispositivos móveis.

Este cenário tem o potencial de trazer benefícios – redução de custos, maior conveniência, melhorias no serviço, facilitação da inclusão financeira e possibilidade de atuação de novos *players*/instituições. No entanto, à medida que o uso de um dispositivo móvel como um instrumento de pagamento de bens e serviços se torna comum, questões relacionadas com a segurança dos dados torna-se um fator crítico e fundamental para a aceitação deste tipo de serviço.

Atendendo à proeminência mundial das soluções *Mobile Payment Services*, impõe-se estabelecer condições mínimas de segurança para a prestação desse serviço de forma a preservar a escolha do consumidor em melhores condições de segurança e aumentar a confiança dos mesmos nos pagamentos móveis.

Com a reforma do quadro regulamentar do Sistema de Pagamentos Cabo-verdiano, o Decreto-legislativo nº 7/2018, de 28 de novembro, veio regular matérias relativas aos princípios orientadores que qualquer sistema de pagamentos a operar no país deve observar, visando a eficiência e a segurança dos mesmos. Um dos princípios elencados no artigo 10º do referido diploma refere-se à definição de políticas e mecanismos de segurança para garantir a confiabilidade operacional num sistema de pagamentos, inclusive no de pagamentos móveis.

O Banco de Cabo Verde prosseguindo no seu papel de regular, fiscalizar e promover o bom funcionamento dos sistemas de compensação e pagamentos, pretende com o presente regulamento estabelecer os requisitos básicos para impulsionar a eficiência e segurança na implementação do *Mobile Payment Services* em Cabo Verde.

Os requisitos são formulados para acomodar a inovação tecnológica e serão revistos, a qualquer momento pelo Banco de Cabo Verde, identificadas novas ameaças ou situações não previstas neste regulamento.

E neste sentido, ao abrigo do n.º 4 do artigo 17º do Decreto-legislativo nº 7/2018, de 28 de novembro, o BCV determina o seguinte:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1º

Objeto

O presente Aviso estabelece os requisitos de segurança, mínimos e comuns, aplicáveis à segurança dos pagamentos efetuados através de dispositivos móveis e que devem ser observados pelos Prestadores de Serviços de Pagamento (PSP), não afetando com isso a sua responsabilidade em matéria de controlo, avaliação de riscos envolvidos nas operações de pagamento e o estabelecimento de uma política de segurança própria que contemple medidas de gestão de incidentes e planos de contingência e continuidade do próprio negócio.

Artigo 2º

Âmbito

1. O disposto no presente Aviso é aplicável:

a) Aos sistemas de pagamentos a operar no país, que prestam serviços de pagamento através de dispositivos móveis;

b) Aos prestadores de serviços de pagamento através de dispositivos móveis.

2. Para efeitos do presente Aviso, entende-se por *Mobile Payment*, os pagamentos para os quais os dados e a instrução de pagamento são transmitidos e/ou confirmados através de comunicação móvel, utilizando um dispositivo móvel.

3. Não são considerados pagamentos móveis para efeitos do presente Aviso:

a) Pagamentos em que o dispositivo móvel é usado apenas para efeitos de acesso e autenticação de transações *online* no site ou no aplicativo de numa instituição financeira;

b) Tecnologias que transformam dispositivos móveis em dispositivos de aceitação de pagamentos por cartão físico (por exemplo, um terminal POS);

c) *Sticker Solutions* (aplicação de um chip adesivo habilitado com tecnologia NFC ao dispositivo móvel). Tendo em conta que os adesivos não interagem de facto com o dispositivo móvel, estas soluções são consideradas serviços de pagamento com cartão sem contato;

d) Operações de pagamento nas condições discriminadas na alínea *l*), nº 2 do artigo 2º do Decreto-legislativo nº 8/2018, de 28 de novembro;

e) Operações de pagamento, tal como definidas na alínea *j*), n.º 2 do artigo 2º do Decreto-legislativo nº 8/2018, de 28 de novembro.

Artigo 3º

Definições

Para efeitos do presente regime jurídico, entende-se por:

a) «Autenticação» procedimento que permite ao prestador de serviços de pagamento verificar a utilização de um instrumento de pagamento específico, designadamente os dispositivos de segurança personalizados;

b) «Autenticação forte» procedimento de autenticação do cliente baseado no uso de dois ou mais dos seguintes elementos - conhecimento, propriedade e inerência: (i) algo que apenas o usuário conhece (por exemplo, login e senha); (ii) algo que apenas o usuário possui (por exemplo, um *token*,); e (iii) algo que o usuário é (por exemplo, uma característica biométrica, como uma impressão digital);

c) «Beneficiário» pessoa singular ou coletiva que seja o destinatário previsto dos fundos que foram objeto de uma operação de pagamento;

d) «Conta de pagamento» conta detida em nome de um ou mais utilizadores de serviços de pagamento, que seja utilizada para a execução de operações de pagamento;

e) «Contrato quadro» contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento;

f) «Cartão SD» cartão *Secure Digital* ou SD é um formato de cartão de memória não volátil para uso em dispositivos portáteis;

g) «Dados confidenciais de pagamento» dados que podem ser usados para realizar fraudes, incluindo dados que permitem que uma ordem de pagamento seja iniciada (por exemplo, PAN, data de vencimento do cartão, CVV2), dados usados para autenticação (identificadores do cliente, data de nascimento, senhas, códigos, PIN, perguntas secretas, senhas / códigos para redefinição, número de telefone), dados usados para pedidos de instrumentos de pagamento ou ferramentas de autenticação a serem enviadas aos clientes (endereço físico do cliente, número de telefone, endereço de e-mail);

h) «Dispositivo Móvel» máquina portátil com as seguintes caraterísticas: (i) conectada a outros dispositivos ou sistemas através de tecnologias de rádio ou via redes de telecomunicações baseadas em tecnologia sem fio; (ii) projetado com uma interface multimídia para interação do usuário (por exemplo, teclado, alto-falante de som); (iii) equipado com uma instalação de armazenamento de dados (por exemplo, um cartão SIM,); e (iv) equipado com um sistema operacional móvel;

i) «Incidentes graves» incidentes associados a funções vitais de negócio, com o maior grau de impacto entre os níveis previstos para a priorização de incidentes nos serviços de tecnologia de informação;

j) «Instrumento de pagamento» qualquer dispositivo personalizado ou conjunto de procedimentos acordados entre o utilizador e o prestador do serviço de pagamento e a que o utilizador de serviços de pagamento recorra para emitir uma ordem de pagamento;

k) «NFC – *Near Field Communication*» tecnologia sem fios que permite a troca de informações entre dispositivos quando estes estão em contacto, sem qualquer necessidade de configurações adicionais. Nos telemóveis com antena/sensor NFC, esta é ativada no mesmo local onde se configuram as outras opções de comunicação como seja o Bluetooth ou o Wi-Fi;

l) «Ordem de pagamento» qualquer instrução de pagamento dada por um ordenante ou um beneficiário ao seu prestador de serviços de pagamento requerendo a execução de uma operação de pagamento;

m) «Ordenante» pessoa singular ou coletiva que detém uma conta de pagamento e que autoriza uma ordem de pagamento a partir dessa conta, ou, na ausência de conta de pagamento, a pessoa singular ou coletiva que emite uma ordem de pagamento;

n) «Prestador de serviços de pagamento» entidades autorizadas a exercer a atividade de prestação de serviços de pagamento a título profissional, nos termos da lei aplicável e respetiva regulamentação do Banco de Cabo Verde;

o) «Serviços de pagamento» atividades enumeradas no nº 1 do artigo 2.º do Decreto-legislativo nº 8/2018, de 28 de novembro, considerando as exclusões previstas no n.º 2 do mesmo artigo.

Artigo 4º

Princípios gerais de segurança

1. Os Prestadores de Serviços de Pagamentos Móveis a operar no país devem reger-se pelos seguintes princípios:

a) Implementar políticas claras de segurança que definem as funções e responsabilidades dos intervenientes e mecanismos que visam garantir a segurança e a confiabilidade operacional, em conformidade com a alínea *d*) do nº 1 do artigo 10º do Decreto-legislativo nº 7/2018, de 28 de novembro;

b) A conceção do *Mobile Payment Service* deve ser baseada numa abordagem integrada de deteção, avaliação permanente e mitigação dos riscos associados e inerentes ao tipo de negócio;

c) Os serviços prestados através de dispositivos móveis devem prever a implementação de procedimentos robustos de autenticação do cliente, protegendo a confidencialidade dos dados na iniciação ao serviço, bem como o acesso a informações sensíveis dos clientes;

d) A conceção do *Mobile Payment Service* deve ser baseada em mecanismos que permitam a transmissão, processamento ou armazenamento de informações sensíveis de forma segura e íntegra, com definição de políticas e adoção de medidas de prevenção e deteção de alterações, modificações ou adulterações das informações;

e) Os Prestadores de Serviços de Pagamento devem implementar processos fiáveis para a monitorização de transações e sistemas, de forma a identificar-se perfis de pagamentos anormais e prevenir atos fraudulentos;

f) Quando terceiros estiverem envolvidos nos pagamentos móveis prestados, por exemplo as operadoras de redes móveis, os prestadores de serviços de pagamentos devem garantir que os serviços do primeiro sejam fornecidos em conformidade com os requisitos estabelecidos neste Aviso;

g) Os Prestadores de Serviços de Pagamento devem informar e clarificar os clientes sobre as especificações do serviço, disponibilizando mecanismos que permitam a promoção gradual do seu entendimento, contribuindo de forma ativa para o uso dos serviços por parte dos clientes num ambiente de confiança.

2. As disposições descritas neste Aviso constituem exigências mínimas, que não substituem a responsabilidade dos PSP e outros participantes do sistema de pagamento, de monitorizar e avaliar continuamente os riscos envolvidos nos serviços prestados, desenvolver suas próprias políticas de segurança e implementar medidas adequadas de segurança, contingência, gestão de incidentes e continuidade de negócio que sejam proporcionais aos riscos inerentes.

CAPÍTULO II

REQUISITOS DE SEGURANÇA PARA PAGAMENTOS ATRAVÉS DE DISPOSITIVOS MÓVEIS

Artigo 5º

Disposições gerais

Os requisitos de segurança do *Mobile Payment Service* estão organizados e apresentados neste Aviso em três níveis, designadamente:

a) Requisitos de controlo geral de segurança da plataforma de suporte ao serviço de pagamento móvel para a identificação, avaliação, mitigação e gestão de riscos internos e externos associados ao negócio;

b) Requisitos de segurança para os pagamentos móveis, a nível da execução e processamento de transações, começando pelo acesso ao serviço, pela iniciação do pagamento, pela autorização de transações, até à proteção de informação confidencial;

c) Requisitos de informação e sensibilização dos clientes, a nível de proteção do cliente, sua informação e educação sobre os aspetos de segurança subjacentes ao tipo de serviço.

Artigo 6º

Requisitos de controlo geral dos prestadores de serviço de pagamentos móveis

1. Atendendo ao princípio elencado na alínea *d*), do nº 1 do artigo 10º do Decreto-legislativo nº 7/2018, de 28 de novembro, o prestador de serviço de pagamento móvel deve possuir um Manual de Política de Segurança do Serviço, onde se preveja uma clara articulação de funções e responsabilidades que permita impor princípios de segurança, devendo, ainda, ser prevista uma frequência de revisão e respetiva adaptação periódica.

2. A política de segurança deve ainda abordar questões relacionadas com a arquitetura apropriada da solução/aplicativo de pagamento e com a implementação de todos os componentes envolvidos na prestação de um serviço de pagamento móvel, inclusive os riscos inerentes das relações de terceirização de serviços (operadores telecomunicações, fabricantes de dispositivos móveis, desenvolvedores de aplicativos, etc.).

3. O prestador de serviço de pagamento móvel deve elaborar um plano contínuo de gestão de riscos, em conformidade com a alínea c), nº 1 do artigo 10º do Decreto-legislativo nº 7/2018, de 28 de novembro, com o objetivo de garantir a segurança dos pagamentos móveis, principalmente a proteção dos dados confidenciais.

4.O PSP deve realizar e documentar avaliações de risco para os serviços de pagamento oferecidos, tendo em conta:

a) A solução tecnológica utilizada na prestação do serviço – riscos associados às plataformas tecnológicas relevantes, arquitetura dos aplicativos, técnicas de programação e rotinas de operações;

b) Os serviços terceirizados ou fornecidos por provedores externos – riscos associados aos fabricantes de dispositivos móveis, desenvolvedores de aplicativos;

c) O dispositivo móvel dos clientes - riscos associados aos consumidores;

d) O dispositivo de aceitação do pagamento móvel – riscos associados aos utilizadores comerciantes.

5. O prestador de serviço de pagamento móvel deve garantir a monitorização constante e acompanhamento dos incidentes de segurança, incluindo reclamações de clientes relacionadas à segurança.

6. Os PSP devem garantir que o serviço prestado incorpore mecanismos seguros de registo dos dados da transação, incluindo uma referência que permita identificar a operação de pagamento, a data e hora de execução, as alterações de parametrizações e acesso aos dados, permitindo a rastreabilidade das transações em qualquer momento.

7. Os processos implementados e os arquivos de *log* devem ser capazes de identificar e rastrear a fonte através da qual o pagamento foi iniciado (ponto de venda, internet) e o beneficiário do pagamento (comerciante, etc.).

8. Sempre que ocorram incidentes graves que afetem os serviços, alterações relevantes nas infraestruturas ou identificação de novas ameaças, o PSP deve realizar uma revisão dos principais cenários de risco e medidas de segurança existentes.

9. As medidas de segurança para os serviços de pagamentos móveis devem ser auditadas periodicamente para garantir sua robustez e eficácia, proporcionalmente aos riscos de segurança envolvidos.

10. Para efeitos do número anterior, a auditoria deve ser efetuada por entidades confiáveis e baseada numa ótica objetiva e independente, ou seja, os auditores não devem estar envolvidos no desenvolvimento, implementação ou gestão operacional dos serviços de pagamento móvel fornecidos.

11. Sempre que os prestadores de serviços de pagamento móvel terceirizarem funções que possam afetar a segurança dos serviços, o contrato entre as partes deve incluir disposições que exijam a conformidade com os princípios estabelecidos neste Aviso.

Artigo 7º

Requisitos de segurança para os pagamentos via dispositivos móveis

1. Aos serviços de pagamento móvel prestados no país é aplicável o regime jurídico que regulamenta a prestação de serviços de pagamento e a emissão, distribuição e reembolso de moeda eletrónica, nos termos do Decreto-legislativo nº 8/2018, de 28 de novembro.

2. O prestador de serviço de pagamento móvel deve assegurar que as informações e condições fornecidas ao utilizador do serviço de pagamento, previstas no artigo 16º do Decreto-legislativo nº 8/2018, de 28 de novembro, contenham, adicionalmente, as seguintes informações, tratando-se de um serviço de pagamento móvel:

a) Informações claras sobre quaisquer requisitos em termos de equipamento móvel, *software* ou outras ferramentas necessárias;

b) Diretrizes para o uso correto e seguro das credenciais de acesso;

c) Uma descrição passo-a-passo dos procedimentos a seguir pelo cliente no momento de submeter e autorizar uma transação de pagamento, inclusive as consequências de cada ação;

d) Diretrizes para o uso correto e seguro de todo o *hardware* e *software* fornecido ao cliente;

e) Procedimentos a seguir em caso de perda, roubo, apropriação abusiva ou qualquer utilização não autorizada do dispositivo móvel;

f) Procedimentos a seguir em caso de mudança de operador de rede móvel pelo cliente ou aquisição de um novo dispositivo móvel;

g) Descrição das responsabilidades dos intervenientes na prestação e utilização de serviços de pagamento móvel;

3. O prestador de serviço de pagamento móvel deve garantir procedimentos de autenticação forte do cliente, de acordo com a definição fornecida neste regulamento, para autorização de pagamentos.

4. Sem prejuízo do disposto no número anterior, o PSP pode considerar a adoção de medidas de segurança alternativas de autenticação de clientes para os seguintes casos:

a) Nas transferências entre contas de pagamento sediadas num mesmo prestador de serviços de pagamento, mediante uma análise de riscos associados;

b) Nas operações de pagamento de baixo valor, tal como definido no artigo 27º do Decreto-legislativo nº 8/2018, de 28 de novembro;

c) Beneficiários fiáveis previstos numa lista indicada pelo ordenante;

d) Operações recorrentes do mesmo montante e junto do mesmo beneficiário;

e) Transferências a crédito entre contas de pagamento detidas pela mesma pessoa singular ou coletiva.

5. Sempre que o prestador de serviço de pagamento móvel autorizar operações pagamentos de baixo valor com medidas alternativas de autenticação do cliente deve implementar soluções que limitem o risco financeiro para o cliente, como limitar o valor acumulado para pagamentos consecutivos e exigir uma autenticação forte do cliente para o *reset* dos valores acumulados.

6. O prestador de serviço de pagamento móvel deve definir limites nas tentativas de autenticação e estabelecer limites de tempo para a validade de cada autenticação, ou seja:

a) O PSP deve definir o número máximo de tentativas de autenticação com falha, após o qual o acesso ao serviço de pagamento móvel é temporariamente ou permanentemente bloqueado. Devem ser estabelecidos procedimentos seguros para a reativação dos serviços bloqueados;

b) Ao utilizar uma senha única para fins de autenticação, o PSP deve garantir que o período de validade de tais senhas seja limitado ao mínimo necessário.

7. Sempre que uma senha ou PIN é usada como um elemento para realizar a autenticação do cliente, o PSP deve garantir que a sua introdução seja feita de forma a evitar que ela seja comprometida.

8. Ao projetar, desenvolver e manter as soluções de pagamentos móveis, os PSP devem implementar medidas de segurança para garantir que os dados usados pelo aplicativo de pagamento não sejam acessíveis a outros aplicativos/processos do dispositivo móvel.

9. Caso um cliente desejar mudar de operador de rede móvel, o PSP deve garantir que a transferência das credenciais de utilizador do aparelho ou dos dispositivos removíveis (por exemplo, cartão SD, cartão SIM, etc.), para o novo dispositivo seja realizada de forma segura.

10. O prestador de serviço de pagamento móvel deve garantir que os processos de inscrição do cliente e de fornecimento inicial das ferramentas de autenticação e/ou entrega do *software* necessário para a utilização do serviço de pagamento móvel é feita por canais seguros, assegurando que as credenciais entregues ao cliente não sejam intercetadas e reutilizadas.

11. Em conformidade com o previsto no artigo 29º do Decreto-legislativo nº 8/2018, de 28 de novembro, o prestador de serviço de pagamento móvel deve garantir, mediante estipulação expressa no contrato quadro, o direito de bloquear um dispositivo móvel por motivos que se relacionem com a segurança do instrumento. Nesse caso o PSP deve:

a) Estar em posição de desativar remotamente a funcionalidade de pagamento móvel do dispositivo móvel;

b) Fornecer soluções suficientemente seguras que permitam ao cliente desativar/ativar a funcionalidade de pagamento móvel do dispositivo móvel.

12. Em casos de perda ou roubo de dispositivos móveis, o prestador de serviço de pagamento móvel deve garantir a proteção dos dados confidenciais do pagamento e dos dados pessoais do cliente, seja com a possibilidade de desativar o aplicativo de pagamento móvel ou soluções para apagar remotamente os dados confidenciais de um aparelho perdido ou roubado.

13. Sempre que for utilizada tecnologia *contactless* nos pagamentos, o prestador do serviço de pagamento móvel deve assegurar mecanismos de segurança adequados para garantir que dados confidenciais do pagamento ou dados pessoais do cliente não sejam acedidos ou modificados sem autorização.

14. Para mitigar os riscos de contaminação cruzada, o PSP deve garantir que nenhum dado de pagamento confidencial relacionado a pagamentos móveis, incluindo dados de autenticação, como um PIN, possa ser reutilizado para efetuar pagamentos fraudulentos em outros canais (por exemplo, pagamentos via Internet ou cartões falsificados).

Artigo 8º

Requisitos a nível de sensibilização do cliente, educação e comunicação

1. O prestador de serviço de pagamento móvel deve fornecer assistência e orientação aos seus clientes, sempre que necessário, em relação ao uso seguro dos serviços de pagamento móvel.

2. Devem ser fornecidas ao utilizador do serviço de pagamento as seguintes informações quanto aos meios de comunicação com o PSP, através de um canal seguro:

a) O procedimento para os clientes reportarem os pagamentos fraudulentos, incidentes suspeitos ou anomalias durante a prestação de serviços de pagamento móvel;

b) O meio de comunicação para dar resposta às solicitações dos clientes;

c) A forma como o prestador de serviço notificará o cliente sobre possíveis transações fraudulentas ou alertas de ocorrência de ataques.

3. O prestador de serviço pagamento móvel deve promover programas de sensibilização do cliente para a necessidade de proteger os seus dados confidenciais e gerir adequadamente a segurança do seu dispositivo pessoal, através da instalação e atualização de componentes de segurança (antivírus, etc.).

4. O prestador de serviço de pagamento móvel deve notificar os clientes sobre o início do pagamento e fornecer informações atualizadas necessárias para verificar se uma transação de pagamento foi iniciada e/ou executada corretamente, bem como os saldos das contas, de forma segura e confiável.

5. A assistência aos clientes deve ser disponibilizada pelo prestador de serviço de pagamento para todas as questões, reclamações, solicitações de suporte, notificações de anomalias ou incidentes referentes a pagamentos móveis e serviços relacionados.

CAPÍTULO III

DISPOSIÇÕES COMPLEMENTARES E FINAIS

Artigo 9º

Regime supletivo

Em tudo o que não se encontre previsto no presente Aviso é aplicável o Regime Jurídico do Sistema de Pagamentos Cabo-verdiano e o Regime Jurídico dos Serviços de Pagamento e de Emissão da Moeda Eletrónica.

Artigo 10º

Instruções Técnicas

O Banco de Cabo Verde pode emitir instruções que venham a ser consideradas necessárias relativamente a orientações específicas para a aplicação operacional do presente Aviso.

Artigo 11º

Prestação de informações

Os pedidos de esclarecimentos ou notificações no âmbito do presente Aviso deverão ser endereçados ao Departamento de Emissão, Tesouraria e Sistema de Pagamento do Banco de Cabo Verde.

Artigo 12º

Entrada em vigor

Este Aviso entra em vigor no dia seguinte ao da sua publicação.

Gabinete do Governador e dos Conselhos do Banco de Cabo Verde, na Praia, aos 10 de junho de 2021. — O Governador, *Óscar Humberto Évora dos Santos*.

II SÉRIE
BOLETIM OFICIAL

Registo legal, nº 2/2001, de 21 de Dezembro de 2001

Endereço Electronico: *www.incv.cv*

IMPRENSA NACIONAL DE CABO VERDE

Av. da Macaronésia,cidade da Praia - Achada Grande Frente, República Cabo Verde.
C.P. 113 • Tel. (238) 612145, 4150 • Fax 61 42 09
Email: kioske.incv@incv.cv / incv@incv.cv

I.N.C.V., S.A. informa que a transmissão de actos sujeitos a publicação na I e II Série do *Boletim Oficial* devem obedecer as normas constantes no artigo 28º e 29º do Decreto-lei nº 8/2011, de 31 de Janeiro.

Quinta-feira, 17 de junho de 2021

II Série
Número 96

BOLETIM OFICIAL

ÍNDICE

PARTE J

PARTE J

MINISTÉRIO DA JUSTIÇA E TRABALHO

Direção-Geral dos Registos, Notariado e Identificação

Conservatória dos Registos e Cartório Notarial do Porto Novo

Extrato de publicação de sociedade nº 394/2021

CONSERVADORA-NOTÁRIA: ALÍCIA PATRÍCIA DA CRUZ DA LUZ

EXTRATO

Certifico narrativamente para efeitos de publicação, que nesta Conservatória dos Registos e Cartório Notarial, a meu cargo, encontram exaradas as seguintes alterações da sociedade comercial "ED Electronic Solutions – Sociedade unipessoal, Lda", com sede em Armazém, São João Baptista, Santo Antão, matriculada sob o nº 284555304/301672620201008:

Divisão e Cessão de quota

Quota dividida: 250.000$00

Titular: Edney Fortes Gonçalves

Quotas resultantes: 150.000$00; 100.000$00.

Cedente: Edney Fortes Gonçalves

Quota transmitida: 150.000$00

Cessionária: Nélida dos Anjos Lopes Monteiro Fortes

Sócios e quotas

Sócio: Edney Fortes Gonçalves;

Quota: 100.000$00

Sócia: Nélida dos Anjos Lopes Monteiro Fortes

Quota: 150.000$00

Alteração firma/denominação e natureza jurídica

Firma/Denominação para: "ED Electronic Solutions, Lda."

Natureza jurídica para: Sociedade por quotas.

Está conforme.

Conservatória dos Registos e Cartório Notarial do Porto Novo, aos 9 de junho de 2021. — A Conservadora-Notária, *Alícia Patrícia da Cruz da Luz.*

CABO VERDE TELECOM, S.A.

Assembleia Geral

Convocatória nº 21/2021

Assembleia–Geral de Acionistas

Mesa

São convocados os Exmos. Senhores Acionistas da Cabo Verde Telecom, S.A., para a reunião anual ordinária da Assembleia-Geral, que terá lugar no dia 9 de julho de 2021, pelas 09H00, no Hotel Praia Mar, na cidade da Praia, Cabo Verde, com a seguinte Ordem de Trabalhos:

1. Apreciar e deliberar sobre o Relatório de Gestão do Conselho de Administração e as Contas do Exercício de 2020, que incluem as Contas Individuais e Consolidadas e o Parecer do Fiscal Único;

2. Apreciar e deliberar sobre a Proposta de Aplicação dos Resultados do Exercício de 2020;

3. Proceder à Apreciação da Administração e da Fiscalização da Sociedade, nos termos dos artigos 297º, nº 1 – al. *c*) e 344.º, nº 1, alínea *c*) do Código das Sociedades Comerciais;

4. Apresentação do Plano de Atividades da Sociedade para o ano de 2021;

5. Apreciar e deliberar sobre outros assuntos de interesse para a Sociedade.

Todos os documentos estão disponíveis para a consulta dos acionistas na sede da Sociedade, junto do Gabinete do Conselho de Administração, durante as horas normais de expediente. Os acionistas que pretenderem receber os documentos de prestação de contas por correio eletrónico, deverão disponibilizar o seu endereço através do email *suporteca@cvt.cv*.

Nos termos dos artigos 301.º e 302.º, n.º 1 do Código das Sociedades Comerciais, qualquer acionista com direito a voto pode fazer-se representar na referida Assembleia-Geral por qualquer pessoa singular com capacidade jurídica plena, devendo, para tanto, dirigir uma carta, devidamente assinada, ao Presidente da Mesa da Assembleia-Geral, na qual seja especificada: (i) a assembleia em causa, (ii) o dia, (iii) a hora da reunião, (iv) a ordem do dia acima indicada, (v) as indicações sobre consultas dos documentos, (vi) a indicação da pessoa ou pessoas que lhe representará (vii) e a menção de que a (s) pessoa (s) representante (s), caso surgem circunstâncias imprevistas, poderá votar no sentido que julgue satisfazer melhor os interesses dele acionista.

Cabo Verde Telecom, na Praia, aos 15 de junho de 2021. — O Presidente da Mesa, *Simão Monteiro.*

II SÉRIE

BOLETIM OFICIAL

Registo legal, nº 2/2001, de 21 de Dezembro de 2001

Endereço Electronico: *www.incv.cv*

IMPRENSA NACIONAL DE CABO VERDE

Av. da Macaronésia,cidade da Praia - Achada Grande Frente, República Cabo Verde.
C.P. 113 • Tel. (238) 612145, 4150 • Fax 61 42 09
Email: kioske.incv@incv.cv / incv@incv.cv

I.N.C.V., S.A. informa que a transmissão de actos sujeitos a publicação na I e II Série do *Boletim Oficial* devem obedecer as normas constantes no artigo 28º e 29º do Decreto-lei nº 8/2011, de 31 de Janeiro.