Política de Segurança para os Serviços de Pagamento através da Internet

Banco BAI Cabo Verde, S.A.
Edifício "BAICENTER" R/C •Chã D'Areia, Praia • Cabo Verde
Tel.: +238 2602300
Email: bai@bancobai.cv • **Portal:** www.bancobai.cv
C.R.P.C.A.P n.º 2728 • NIF 254746420
Capital Social: 2.092.385.000$00

Índice

1. INTRODUÇÃO

O pagamento através da Internet constitui um dos canais importantes para os clientes do Banco BAI Cabo Verde, doravante denominado por BAICV, oferecendo comodidade e celeridade.

Com o uso crescente de meios de pagamento através da Internet, e num cenário em que há cada vez mais ameaças, questões relacionadas com a segurança destes meios tornam-se um fator fundamental para aceitação dos mesmos.

Neste contexto e em cumprimento com o Aviso n.º 2/2021 do Banco de Cabo Verde (BCV) que estabelece requisitos de segurança para pagamentos efetuados através da Internet, o BAICV, ciente das suas responsabilidades, define a presente política de segurança para os serviços de pagamento através da Internet.

2. ÂMBITO

A presente política aplica-se aos serviços de pagamento através da Internet do BAICV, nomeadamente serviços que permitam realizar quaisquer das seguintes operações através da Internet:

- Transferências através de um portal bancário;
- Débitos diretos;
- Operações de pagamento com cartão à distância, incluindo cartões virtuais;

Operações com moeda eletrónicas, nomeadamente transferências.

A presente política, que estabelece os requisitos aplicáveis à segurança dos serviços de pagamento através da Internet, tem como objetivo a apresentação pela Liderança do BAICV a todas as partes interessadas dos seus compromissos em relação à segurança dos serviços de pagamento através da Internet.

3. REFERÊNCIA

Na elaboração desta política, foram considerados legislação, regulamentação, códigos de conduta e outras boas práticas nacionais e internacionais reconhecidas ao nível dos sectores de atuação do BAICV.

Interno

- Política de Segurança e de Sistemas de Informação
- Política de Privacidade e Proteção de Dados;

- Código de Conduta;
- Política de Continuidade de Negócio;

Externo

- **Lei n.º 121/IX/2021 de 17 de março** que altera o regime jurídico geral de proteção de dados pessoais das pessoas singulares, aprovado pela Lei nº **41/VIII/2013**, de **17 de setembro;**
- **Decreto-lei nº 9/2021 de 29 de janeiro** que aprova o regime jurídico de cibersegurança;
- **Decreto-regulamentar nº 1/2021 de 29 de janeiro** que cria a Equipa de Resposta a Incidentes de Segurança Informática, define as suas funções e estrutura, bem como o seu enquadramento administrativo;
- Requisitos de Sistemas de Gestão de Segurança da Informação - **Norma ISO 27001:2022;**

4. TERMOS E DEFINIÇÕES

Para efeitos da presente política, entende-se por:

- Autenticação: Procedimento que permite a verificação da identidade de um utilizador de serviços de pagamento;
- Autenticação forte do utilizador do serviço de pagamento: Procedimento baseado na utilização de dois ou mais dos seguintes elementos classificados como conhecimento (algo que apenas o utilizador conhece, por exemplo uma palavra-passe estática, um código, um número de identificação pessoal), posse (algo que apenas o utilizador possui, designadamente, um dispositivo de autenticação (token), um cartão inteligente, um telemóvel) e inerência (alguma característica inerente ao utilizador, nomeadamente uma característica biométrica);
- Autorização: Procedimento que verifica se um utilizador de serviços de pagamento ou um PSP (Prestador de Serviços de Pagamento) tem o direito de executar uma determinada ação, por exemplo o direito de transferir fundos ou de ter acesso a dados sensíveis;
- Incidente de segurança dos pagamentos de carácter severo: Incidente que tem ou poderá ter um impacto material sobre a segurança, a integridade ou a continuidade dos sistemas relacionados com pagamentos do banco e/ou a segurança de dados de pagamento sensíveis ou de fundos;

- Análise de risco da operação: 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;
- Encriptação ponto-a-ponto: Encriptação na origem da comunicação, enquanto a desencriptação correspondente ocorre no recetor final;
- Palavra-passe de uso único (One Time Password - OTP): 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;
- Princípio da minimização de dados: Política de recolha do mínimo de informação pessoal necessária para executar uma determinada função;
- Princípio do privilégio mínimo: 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.

5. PRINCÍPIOS ORIENTADORES

5.1. Alinhamento com as Diretrizes Regulatórias

A presente política deve garantir o alinhamento com as recomendações e regulamentação publicada pelo Banco de Cabo Verde (BCV), designadamente

- Aviso n.º 2/2021 do BCV, que estabelece os requisitos mínimos e os conteúdos essenciais aplicáveis à segurança na execução de operações de pagamentos efetuados através de Internet.

5.2. Quadro de Avaliação Global dos Riscos

De modo a garantir que haja mecanismos adequados à gestão, controlo e comunicação dos riscos a que estejam ou possam vir a estar expostos os serviços de pagamento através da Internet, deve ser implementado um quadro de avaliação dos riscos, com instrumentos de gestão de riscos sólidos e adequados ao nível de risco identificado, que lhes permita aferir e monitorar riscos subjacentes aos serviços de pagamento através da Internet.

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.

Os resultados das avaliações de riscos efetuados devem ser submetidos à aprovação pela CE.

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

5.3. Controlo e Mitigação de Riscos

De forma a fazer o controlo e mitigação de riscos associados a serviços de pagamento através da Internet, deve-se assegurar:

a) Princípio do privilégio mínimo e separação de funções, em todas as etapas de implementação dos serviços de pagamentos através de Internet;

b) Princípio da minimização de dados em todas as etapas de implementação dos serviços de pagamentos através de Internet;

c) Implementação de soluções de segurança de proteção contra ataques em redes, servidores e aplicações associados a serviços de pagamentos através de Internet;

d) Testes e/ou auditorias regulares, a serem realizados por especialistas qualificados e independentes internos ou externos, e correção contínua de vulnerabilidades nos sistemas mencionados no item anterior;

e) Identificação clara dos sistemas de prestação de serviços de pagamento através da Internet através de e.g. certificados digitais;

f) Implementação de processos de monitoramento e registo (logs) dos acessos e ações realizadas nos sistemas mencionados anteriormente, de forma a assegurar a rastreabilidade de todas as operações relevantes.

5.4. Monitorização e procedimentos de reporte de incidentes

A monitorização e o tratamento dos incidentes de segurança relacionados com os serviços de pagamento através da Internet devem ser assegurados. Reclamações dos utilizadores destes serviços devem ser incluídas, devendo-se para tal:

- Adotar procedimentos de reporte de incidentes de segurança relevantes para a CE e, em caso de incidentes de segurança dos pagamentos graves (e.g. suspeitas de fraudes resultando na movimentação de valores a débito ou a crédito), às autoridades de supervisão e de proteção de dados caso necessário;

- Fazer o tratamento e acompanhamento contínuos de incidentes de segurança e reclamações de utilizadores de serviços de pagamento relacionadas com a segurança.

5.5. Mecanismos de Controlo Específicos e Medidas de Segurança

Os seguintes itens específicos devem ser garantidos em relação aos serviços de pagamento através da Internet:

a) Os utilizadores de serviços de pagamento devem ser devidamente identificados, garantindo o cumprimento de processos de identificação e verificação, 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;

b) Fornecimento antecipado e regular de todas as informações necessárias aos utilizadores, incluindo requisitos, procedimentos e regras para a utilização segura e riscos associados, em conformidade com a legislação cabo-verdiana relativa a serviços de pagamento;

c) O contrato de utilização dos serviços deve explicitar responsabilidades e obrigações e indicar a possibilidade de bloqueio de operações por razões de segurança ou compliance;

d) Os sistemas deverão garantir uma autenticação forte do utilizador do serviço de pagamento, sendo que medidas alternativas de autenticação devem ser adotadas para casos excecionais;

e) Disponibilização de forma segura do primeiro pedido de instrumentos/ferramentas de autenticação, garantindo-se um ambiente seguro e de confiança para a realização desta ação, procedimentos seguros e mecanismos que permitam a verificação de autenticidade;

f) Limitação de número de tentativas de autenticação após o qual o acesso é bloqueado e procedimentos seguros para a reativação, tempo limite de sessões e limites temporais para a validade da autenticação, terminando sessões inativas, incluindo palavras-passe de uso único (OTP);

g) Proteção de forma adequada contra roubo e acesso ou alteração não autorizada de dados sensíveis durante o armazenamento, tratamento ou transmissão, devendo-se fazer uso de encriptação segura ponto-a-ponto, salvaguardando confidencialidade e integridade.

5.6. Sensibilização, Educação e Comunicação com o Utilizador

De forma a instruir e a apoiar os utilizadores de serviços de pagamento através da Internet, deve-se:

a) Assistir e orientar os utilizadores em relação à utilização segura dos serviços de pagamento através da Internet e em relação a questões, reclamações, pedidos de apoio e notificações de anomalias ou incidentes relacionados sempre que necessário;

b) Comunicar com os seus utilizadores de forma a tranquilizá-los sobre a autenticidade das mensagens recebidas;

c) Disponibilizar um canal seguro de comunicação, informar os utilizadores da existência do mesmo e alertar sobre falsas comunicações a partir de outros canais;

d) Explicar aos utilizadores os procedimentos de reporte em caso de suspeitas de fraude ou outras ações ilícitas e procedimentos seguintes, nomeadamente respostas ou notificações do Banco;

e) Manter os utilizadores informados acerca dos procedimentos utilizando um canal seguro;

f) Alertar os utilizadores sobre riscos emergentes significativos utilizando um canal seguro;

g) Sensibilizar os utilizadores sobre a proteção de suas palavras-passe, tokens, informações pessoais e outros dados confidenciais, segurança do dispositivo, ameaças e riscos significativos e website/software genuíno;

h) Prover serviços de alerta e gestão de perfil de utilizador e definir limites aplicáveis aos serviços de pagamento através da Internet (e.g. montante máximo de transferência);

i) Permitir que utilizadores desativem funcionalidade de pagamento através da Internet;

j) Fornecer aos utilizadores informações sobre o estado de execução de pagamentos, incluindo possibilidade de verificação se a operação foi iniciada e/ou executada corretamente, e sobre saldos das contas quase em tempo real;

k) Fornecer demonstrações eletrónicas detalhadas num ambiente seguro e de confiança (e.g. após execução de uma operação ou periódicos). Canais como SMS ou e-mail devem ser utilizados, não devendo ser incluídos dados sensíveis;

5.7. Relação com Outras Entidades

Em caso de contratos celebrados com outras entidades relativos a serviços de pagamentos através da Internet, deve-se garantir a inclusão de cláusulas que obrigam ao cumprimento dos itens mencionados nesta política.

6. RESPONSABILIDADE E ATRIBUIÇÕES

a) **Conselho de Administração (CA)** – Órgão social composto por administradores executivos e não-executivos do Banco responsável, no âmbito das suas funções, pela aprovação da presente política.

b) **Comissão Executiva (CE)** - Órgão de gestão corrente do Banco responsável, no âmbito das suas atribuições, pela aprovação dos normativos, pela promoção da implementação da presente política e seu contínuo aprimoramento suportado por recursos apropriados para alcançar os objetivos estabelecidos e pela aprovação dos resultados das avaliações de riscos associados a serviços de pagamento através da Internet.

c) **Comissão de Supervisão de Gestão de Risco (CSGR)** – Órgão de supervisão e controlo, encarregue de auxiliar e aconselhar o Conselho de Administração (CA) no que respeita à estratégia de gestão dos riscos do Banco.

d) **Comissão de Supervisão de Controlo Interno (CSCI)** – Órgão de supervisão e controlo, encarregue de auxiliar o Conselho da Administração (CA) na supervisão geral e fiscalização do controlo interno, auditoria e conformidade com as políticas, normas e requisitos do negócio.

e) **Direção Tecnologias de Informação (DTI)** – Unidade de estrutura responsável, no âmbito das suas atribuições, pela implementação dos requisitos técnicos de segurança associados a sistemas de prestação de serviços de pagamento através da Internet, bem como pela custódia dos dados de pagamento sensíveis.

f) **Direção de Segurança de Informação (DSI)** – Unidade de estrutura responsável, no âmbito das suas atribuições, pela avaliação dos requisitos técnicos de segurança e pela monitorização, acompanhamento

e reporte dos incidentes de segurança referentes a serviços de pagamento através da Internet, bem como pela implementação de um quadro de avaliação de riscos que permita aferir e monitorar riscos subjacentes aos serviços de pagamento através da Internet.

g) **Gabinete de Gestão de Risco (GGR)** – Unidade de estrutura responsável, no âmbito das suas atribuições, por assistir o CA na definição da estratégia de risco do Banco, bem como na conceção, implementação e monitorização do Modelo de Gestão de Risco.

h) **Direção de Banca Digital (DBD)** – Unidade de estrutura responsável, no âmbito das suas atribuições, pela conceção, desenvolvimento e gestão dos cartões e dos sistemas de pagamento, bem como pela evolução contínua, inovação e segurança de todos os canais digitais do Banco.

i) **Gabinete de Auditoria Interna (GAI)** - Unidade de estrutura responsável, no âmbito das suas atribuições, pela realização de ações de auditoria, de forma a assegurar o controlo e cumprimento das orientações, processos e procedimentos relacionados com a segurança dos serviços de pagamento através da Internet e demais normativos aplicáveis.

j) **Direção Comercial (DCM)** - Unidade de estrutura responsável, no âmbito das suas atribuições, pela realização de ações de sensibilização, educação e comunicação com os utilizadores dos serviços de pagamento através da Internet e demais normativos aplicáveis.

k) **Gabinete Marketing e Comunicação (GMC)** - Unidade de estrutura responsável, no âmbito das suas atribuições, pela realização de ações de sensibilização, educação e comunicação com os utilizadores dos serviços de pagamento através da Internet e demais normativos aplicáveis.

Unidades de Estrutura (UE) - responsáveis, no âmbito das suas atribuições, pela colaboração na implementação e operacionalização da presente política.

7. INCUMPRIMENTO

O incumprimento dos princípios orientadores descritos na presente política pelos Colaboradores do BAICV, será considerado como uma violação das normas internas do Banco.

Como tal, a inobservância do conteúdo desta política, constituirá sempre uma infração disciplinar para colaboradores internos ou contratual para entidades externos, sem prejuízo da responsabilidade civil ou criminal

que ocorra no caso, ficando o colaborador, ou entidade contratada em causa sujeita aos procedimentos legais e disciplinares que se mostrem adequados e aplicáveis às circunstâncias apuradas.

8. REVISÃO E ATUALIZAÇÃO

A presente política deve ser revista sempre que se considera desadequado em cumprimento da legislação ou regulamentação interna ou externa, e respeitando o tempo previsto para atualização definido no BAICV. Qualquer alteração ou revisão desta política deverá ser submetida ao Conselho de Administração para aprovação.

9. DIVULGAÇÃO E PUBLICAÇÃO

A presente política é objeto de divulgação através da intranet e disponibilizada igualmente em outros canais definidos para comunicação do Banco.