



Agência de Pagamentos de Angola, Lda.

RESUMO POLÍTICA DE SEGURANÇA CIBERNÉTICA

DIRECÇÃO DE COMPLIANCE
REALTRANSFER – AGÊNCIA DE PAGAMENTOS DE ANGOLA, LDA

Referência: Política Segurança Cibernética
Versão: 2.0
Data entrada em vigor: Março 2024

Índice

1. Introdução	3
2. Enquadramento Institucional	4
3. Objectivo	4
4. Princípios	5
5. Perfil de Risco	5
6. Medidas Implementadas para Segurança das Informações Sensíveis	6
7. Segurança dos Processos de Pagamento	7
8. Acesso Interno	7
9. Identificação e Autenticação	8
10. Palavras-Passe	8
11. SEGURANÇA DA INFORMAÇÃO	8
12. Cópias de Segurança e Recuperação de Dados	9
13. SEGURANÇA NA UTILIZAÇÃO DOS SISTEMAS INFORMÁTICOS	9
14. Gestão de Incidente	9
15. Processo de Comunicação ao Regulador	9
16. Continuidade de Negócio	9
17. Promulgação	9

1. Introdução

A Política de Segurança Cibernética da RealTransfer – Agência de Pagamentos de Angola (“RealTransfer”), Lda. visa garantir o cumprimento normativo interno da organização, de forma a dar cumprimento as exigências legais da entidade supervisora, o Banco Nacional de Angola (“BNA”) presentes no Aviso n.º 08/2020 de 2 de Abril, Aviso n.º 02/2022 de 2 de Fevereiro e Instrutivo nº 10/2020, de 29 de Maio.

A Segurança Cibernética tem como principais objectivos garantir os níveis adequados de integridade, autenticidade, disponibilidade e confidencialidade requeridos para a protecção da informação gerida pela RealTransfer.

A Política de Segurança Cibernética da RealTransfer constitui uma base comum a todos os Departamentos, permitindo a adopção de padrões de segurança organizacional, de práticas eficazes na gestão da segurança da informação e fornecendo confiança nas relações inter-organizacionais que envolvam a Instituição.

As regras previstas na presente Política são aplicáveis a todos os colaboradores da RealTransfer, incluindo também todos os colaboradores de empresas suas prestadoras de serviços, assim como as próprias empresas que estão vinculadas através dos respetivos contratos de prestação de serviços. Deste modo, todas as pessoas e entidades acima referidas estão obrigadas a cumprir e fazer cumprir as regras estabelecidas no presente documento.

A RealTransfer, através da presente política, compromete-se com a gestão eficaz da segurança cibernética e dos activos pelos quais é responsável, em concordância com os objectivos estratégicos da empresa e a legislação em vigor.

Os procedimentos e a Política de Segurança Cibernética estão sujeitos à aprovação do Conselho de Gerência.

2. Enquadramento Institucional

REAL TRANSFER - Agência de Pagamentos de Angola, Limitada, Instituição Financeira não bancária, autorizada pelo Banco Nacional de Angola em 15 de Maio de 2008 e registada neste Banco sob o n.º 400, com sede na Avenida Comandante Valódia, n.º26, em Luanda, NIF 5417028959, registada na Conservatória do Registo Comercial de Luanda sob o número 1.122-08 e com o capital social de Kz. 80.000.000 (Oitenta Milhões de Kwanzas).

3. Objectivo

A presente Política é aplicável a todos os colaboradores da RealTransfer, tendo todos os colaboradores a responsabilidade de serem pertinazes no seu pleno cumprimento.

Ao abrigo do artigo nº. 7 do Aviso 08/2020, a RealTransfer tem na sua estrutura interna um equipa/área dedicada à política de segurança cibernética, sendo esta responsável pela prevenção, detecção e redução de vulnerabilidades e impactos gerados pelos incidentes relacionados ao ambiente cibernético que afetem a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação e pela execução do plano de acção e de resposta a incidentes.

Desta forma, a RealTransfer compromete-se a:

- Cumprir os requisitos legais nacionais e internacionais em matéria de gestão de dados sensíveis de pagamento dos nossos clientes;
- Garantir a confidencialidade, integridade e disponibilidade da informação nos seus processos;
- Assegurar a comunicação efectiva das políticas e procedimentos em matéria de segurança cibernética;
- Implementar um processo contínuo de sensibilização e formação;
- Demonstrar uma organização segura em matéria de protecção dos dados sensíveis de pagamento dos nossos clientes;
- Obter o consentimento explícito da pessoa para utilização dos seus dados pessoais de pagamento;
- Nos termos da legislação em vigor a RealTransfer efectua o tratamento dos dados para cumprir as suas obrigações e os seus direitos, bem como os das pessoas, em matéria de

legislação laboral, de segurança social e de proteção social.

4. Princípios

A Segurança da Informação Cibernética deve abranger quatro aspetos:

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente pelas pessoas autorizadas;
- **Integridade:** garantia de que a informação seja mantida no seu estado original visando protegê-la contra alterações indevidas, intencionais ou acidentais.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos activos correspondentes sempre que necessário.
- **Autenticidade:** garantia da identidade dos usuários que enviam a informação, isto significa que o não-repúdio é assegurado quando há a certeza de que o remetente não pode negar a autoria da mensagem.

5. Perfil de Risco

Para determinar o perfil de risco de uma instituição, é necessário ter em conta que as diferentes áreas funcionais têm um contributo distinto para a actividade global da instituição. Cada área de negócio é ponderada com base em critérios quantitativos, como a sua contribuição percentual para os resultados financeiros. No entanto, outros factores, como as perspectivas de crescimento, a volatilidade dos resultados e a importância da área para a reputação da instituição, podem justificar a atribuição de pesos adicionais, mesmo que o impacto quantitativo seja menor.

A determinação do perfil de risco da RealTransfer requer uma avaliação abrangente dos riscos decorrentes das actividades realizadas pela instituição, juntamente com uma análise dos mecanismos de governação interna. Esta avaliação inclui aspectos relacionados com a organização, gestão e processos de controlo implementados para mitigar os riscos associados.

É crucial considerar o histórico da instituição no sector e a sua actividade financeira ao avaliar os riscos aos quais ela está ou poderá estar exposta. Isso proporciona perspectivas valiosas para compreender melhor os desafios e oportunidades enfrentados pela instituição no seu ambiente operacional.

A RealTransfer dedica-se activamente à formação contínua dos seus colaboradores e à monitorização constante de resultados e ferramentas. Este compromisso permite antecipar e prever os riscos, garantindo que sejam tomadas as medidas necessárias para mitigar potenciais danos significativos.

Considerando que a RealTransfer se dedica exclusivamente à atividade de remessas de valores de Angola para o exterior, e que cumpre rigorosamente as limitações de valores estabelecidas e regulamentadas pelo supervisor BNA, além de implementar todas as medidas de mitigação recomendadas pela instituição é evidente que o perfil de risco da RealTransfer é baixo.

A RealTransfer concentra-se principalmente na realização de remessas de valores de e para o estrangeiro, um serviço exclusivamente oferecido de forma presencial aos clientes. Esta abordagem elimina a necessidade de utilização de serviços de pagamento online e móveis, o que, por sua vez, minimiza a exposição da RealTransfer aos riscos associados à utilização da internet.

É fundamental ressaltar que as remessas de valores de Angola para o exterior estão sujeitas a limitações específicas, conforme estabelecido no Instrutivo n.º 06/2022, de 24 de Junho de 2022 do Banco Nacional de Angola (BNA). Segundo este instrutivo, as remessas estão limitadas a 5 mil dólares ou ao equivalente em outra moeda estrangeira, por mês e por ordenador.

A gestão e o acompanhamento desta política são realizados pela gerência da RealTransfer, levando em consideração a dimensão da empresa, seu modelo de negócio, perfil de risco e natureza das operações, assim como a complexidade dos produtos, serviços, actividades e processos, além da sensibilidade dos dados e informações.

6. Medidas Implementadas para Segurança das Informações Sensíveis

Esta secção Detalha as medidas adotadas para proteger os dados sensíveis dos clientes, abrangendo a recolha, classificação e tratamento dessas informações.

A RealTransfer possui somente um canal onde é possível realizar transferências e pagamentos:

- Presencialmente – através da nossa rede de agências;

Sendo a RealTransfer uma Instituição de Pagamento, sujeita à legislação em matéria de Prevenção e Combate ao Branqueamento de Capitais, do Financiamento do Terrorismo e da Proliferação de Armas de Destrução em Massa, nomeadamente, no âmbito da Lei n.º 05/20 de 27 de Janeiro, encontra-se autorizada a realizar os tratamentos de dados pessoais necessários ao cumprimento dos deveres preventivos.

O tratamento dos dados pessoais tem como finalidade exclusiva a prevenção do branqueamento de capitais e do financiamento do terrorismo, não podendo tais dados ser posteriormente tratados para quaisquer outros fins, incluindo fins comerciais.

7. Segurança dos Processos de Pagamento

A RealTransfer não possui plataformas onde seja possível realizar operações de pagamento através de sítios electrónicos. Dispõe, apenas, de um canal de pedido de realização de transferências, presencialmente.

O pedido de realização de operações de pagamento, quando feito presencialmente, é executado por colaboradores da RealTransfer, devidamente autorizados a aceder aos sistemas informáticos da RealTransfer e de acordo com a política de gestão de acessos da RealTransfer.

O cliente não tem forma de aceder/consultar/executar operações por si pretendidas ou já efectuadas, sendo que, para ter conhecimento do estado/situação da operação de pagamento terá sempre que consultar colaboradores da RealTransfer, através do serviço de apoio ao cliente através do e-mail: info@realtransfer.com ou via telefónica, através do número (+244) 929 333 001.

Não existe utilização externa dos dados recolhidos para autenticação de clientes.

8. Acesso Interno

A RealTransfer dispõe de vários mecanismos de controlo de acesso físico e lógico, para proteger os sistemas informatizados.

O sistema informático da RealTransfer, tem um sistema de controlo de rastreabilidade através de tabelas de auditoria que permitem ter um controlo e rastreabilidade dos colaboradores. Esta informação é passível de exportação para controlo detalhado através da ferramenta do aplicativo Trader.

Esses dados apenas podem ser verificados por determinados utilizadores, com permissões específicas.

9. Identificação e Autenticação

O sistema informático utilizado pela RealTransfer, a nível de *FrontOffice* e de *BackOffice*, para registo de operações dos clientes e tratamento de dados do mesmo, é o sistema informático TRADER.

Todos os utilizadores dos sistemas de informação da RealTransfer são identificados de forma única e exclusiva de acordo com o perfil respetivo, permitindo, assim, o controlo do acesso aos recursos disponibilizados pelo sistema Trader, como computadores, servidores e recursos locais da rede.

10. Palavras-Passe

A RealTransfer tem instituídas práticas de definição de palavras-passe, nomeadamente no que respeita à sua definição, retenção e expiração de senhas seguras, garantindo a proteção dos dados de utilizador.

11. SEGURANÇA DA INFORMAÇÃO

Apresenta os activos de informação e a classificação da informação, sublinhando a importância de proteger todos os tipos de informação manipulada pela RealTransfer.

Informação tratada pela RealTransfer encontra-se classificada em 5 níveis, seja no âmbito de recolha, de tratamento, transferência ou destruição e é tratada em conformidade. O tratamento e classificação de informação apresenta a seguinte estrutura:

- I. Muito Confidencial
- II. Confidencial
- III. Reservada
- IV. Interna
- V. Pública

A definição dos perfis de acesso aos diversos tipos de informação encontra-se explanada em documento próprio de definidos perfis de acesso, cuja atribuição varia consoante o tipo de informação que é necessária para o desempenho da função de cada colaborador.

12. Cópias de Segurança e Recuperação de Dados

A RealTransfer implementou práticas de backup e recuperação de dados para garantir a continuidade dos serviços em caso de incidentes.

13. SEGURANÇA NA UTILIZAÇÃO DOS SISTEMAS INFORMÁTICOS

Estão implementados procedimentos de gestão e uso responsável de equipamentos, incluindo postos de trabalho, equipamentos portáteis e a utilização da internet e do correio eletrónico.

14. Gestão de Incidente

Detalha o processo de gestão de incidentes cibernéticos, desde a identificação e verificação até a resolução e classificação da criticidade.

15. Processo de Comunicação ao Regulador

Explica o procedimento para comunicar incidentes significativos ao Banco Nacional de Angola, incluindo os prazos para reporte inicial, intercalar e final.

16. Continuidade de Negócio

A RealTransfer possui um processo de continuidade de negócios que foi desenvolvido com o objectivo de minimizar os impactos e perdas de activos de informação após a ocorrência de um incidente crítico, garantindo que os níveis de impacto sejam aceitáveis.

17. Promulgação

A versão actual da Política de Segurança Cibernética foi aprovada em reunião do Conselho de Gerência do dia 19 de Março de 2024 e entra em vigor no dia da sua promulgação.