Versão 0.1/2022

PRIME SOLUTIONS, S.A.

SOCIEDADE CORRECTORA DE VALORES MOBILIÁRIOS

Política de Segurança de Informação e Comunicação

PRIME SOLUTIONS
CORRECTORA DE VALORES MOBILIÁRIOS

ÍNDICE

1. Enquadramento

A PRIME SOLUTIONS – SOCIEDADE CORRECTORA DE VALORES MOBILIÁRIOS, SCVM, é uma instituição financeira não bancária, de direito angolano, que actua no mercado de capitais, cujo objecto consiste na prestação de serviços multidisciplinares no segmento da intermediação financeira e de valores mobiliários, nomeadamente a transmissão de ordens por conta de outrem, a execução de ordens por conta de outrem em mercados regulados ou fora deles, a gestão de carteiras discricionárias e de organismos de investimento colectivos, consultoria de investimentos, elaboração de estudos e análise financeira, registo, depósito e serviços de guarda de valores mobiliários, colocação sem garantias em ofertas públicas e demais *expertises* que entendemos serem relevantes para agregação de valor para os nossos parceiros e que respeitem a legislação angolana para o sector.

Dentro da nossa missão institucional, contribuímos para uma cultura de excelência e proficiência, privilegiando um ambiente de negócio transparente e concorrencial aos nossos clientes e ao mercado, em geral. Neste sentido e face e disposições combinadas da Lei nº 22/15 – Código de Valores Mobiliários e da Lei nº 14/21 – Regime Geral das Instituições Financeiras, da **Lei nº 22/11 de 17 Junho - Protecção de Dados Pessoais**, da **Lei nº 07/17 de 16 Fevereiro - Protecção das Redes e Sistemas Informáticos**, da Lei nº 7/17 de 16 Fevereiro - Protecção das Redes e Sistemas Informáticos o Conselho de Administração, dentro das suas competências e atribuições, implementa a presente Política de Conflito de Interesses, como pilar de todo o processo de relacionamento institucional entre os Colaboradores da nossa Instituição, membros do Conselho de Administração, Conselho Fiscal, Partes Relacionadas, Contrapartes e outras partes interessadas

2. Âmbito

A presente política aplica-se a todos os trabalhadores e partes relacionadas da Prime Solutions, S.A, em todas matérias relacionadas a protecção de dados, sistemas informáticos e informações.

3. Objectivo

Adoptar um conjunto de procedimentos com vista a protecção de todos os dados e informações produzidas na Prime Solutions, S.A, e com as partes com as quais se relaciona e reforçar o compromisso em actuar com os mais elevados padrões de compliance, integridade, ética e governança corporativa na realização dos seus objectivos de negócio e estabelecer uma política institucional de cooperação com as instituições públicas de supervisão e fiscalização do mercado, bem como com as empresas privadas com as quais estabelecemos relações de negócio.

Esta política é, igualmente, um instrumento de suporte a gestão do risco de branqueamento de capitais e crimes subjacentes a este e permite o cumprimento os procedimentos legais estabelecidos na Lei nº 5/20 e toda a regulamentação conexa, sempre que se julgarem necessárias a prevenção e detecção de acções conducentes a esta categoria criminal.

Artigo 1º - Conceitos chave

Segurança Cibernética: conjunto de políticas e controlos, meios e tecnologias que visam proteger programas, computadores, redes e dados de intrusão ilícita ou ataques digitais que provoquem danos aos mesmos.

Computação em Nuvem: modelo que permite o acesso e o fornecimento de forma conveniente e directa a um conjunto de recursos computacionais configuráveis e armazenamento de dados que podem ser rapidamente aprovisionados e acessíveis com o mínimo esforço de gestão ou interacção entre os prestadores de serviços.

Acesso condicionado: sujeição do acesso a um serviço mediante uma assinatura ou qualquer outra forma de autorização individual.

Activos de informação: toda a informação com valor para a Organização, incluindo tecnologias de informação, instalações e pessoas que transmitam, armazenam e processam essa informação, independentemente do seu formato

Cibercrime: crime cometido com recurso aos sistemas electrónicos e novas tecnologias de informação e comunicação.

Incidente de Segurança da Informação: qualquer ocorrência que afecte ou venha a afectar a confidencialidade, integridade e/ou disponibilidade da informação ou das tecnologias de informação, com prejuízo financeiro, reputacional ou operacional para o Banco, incluindo qualquer acção ou omissão, deliberada ou não, que viole a regulação de segurança e privacidade da informação.

Código de acesso: dados ou senha que permite aceder, no todo ou em parte e sob forma inteligível, a um sistema informático.

Segregação de Funções: separação efectiva entre actividades incompatíveis ou conflituantes entre si ou divergentes, visando o controlo no acesso a dados e informação.

Dados: qualquer representação de factos, vídeos, ou imagens, informações ou conceitos, incluindo de programas de computador, que são armazenados, transmitidos ou processados num sistema de informação.

Infraestrutura Tecnológica Crítica: sistemas e activos de informação, sejam físicos, virtuais e vitais para o funcionamento normal das Instituições Financeiras, cuja incapacidade ou destruição acarreta um elevado impacto na operacionalidade das Instituições.

Firewall: dispositivo de rede de computadores, utilizado para aplicar uma política de segurança a um determinado ponto da rede.

Virtual Private Network (VPN): acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

Software: unidade lógica (digital/comunicação), com instruções e dados processados nos servidores e computadores.

Backup: cópia de dados e informações de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.

Colaboradores: toda pessoa singular que presta serviços de natureza não eventual (efectiva) à Prime Solutions, S.A, mediante contraparidas pecuniárias decorrentes de um contrato de natureza laboral.

Subcontratação/Outsourcing: acto de adjudicação de um contrato/serviço, a qualquer pessoa singular, colectiva ou entidade sem personalidade jurídica para que esta actue, de forma directa ou indirecta, por conta da Prime Solutions, S.A, ou em sua substituição.

Activos: fundos, activos financeiros, recursos económicos ou outros bens de qualquer natureza, corpóreos ou incorpóreos, móveis ou imóveis, tangíveis ou intangíveis, documentos ou outro instrumentos legal que comprovem os direitos os bens relativos.

Autoridades de supervisão e fiscalização: entidades cujas funções visam garantir o acompanhamento e controlo da actividade das entidades sujeitas no domínio da prevenção e combate ao branqueamento de capitais, do financiamento do terrorismo e da proliferação de armas de destruição em massa.

Due Diligence: procedimento sobre o qual é despoletado um conjunto de acções, preventivas, com vista a verificar e validar o conjunto de informações submetidas pelos parceiros de negócio, clientes, accionistas e colaboradores da Prime Solutions, S.A, com vista a assegurar a idoneidade destas informações e entidades.

Partes relacionadas: sócios, accionistas com participações qualificadas, entidades pertencentes a grupos económicos, pessoas com relação de cônjuge, descendente ou ascendente, de primeiro e segundo graus, com membros dos órgãos de administração e fiscalização das instituições financeiras, considerados directamente ou como beneficiários últimos das transacções ou dos activos.

Artigo 2º - Directrizes operacionais

1. No âmbito da presente política, os procedimentos abaixo descritos representam os critérios de segurança de dados e sistemas de informação implementados, de acordo com a dimensão, o perfil de risco, modelo de negócio e das operações da Prime Solutions, S.A, bem como em consideração aos produtos, serviços, actividades e processos, dando primazia ao registo e arquivo de informação.

2. Os procedimentos e os controlos adoptados permitem reduzir a vulnerabilidade da Prime Solutions, S.A, a incidentes de cibercrimes, com base no quadro regulamentar vigente.

Artigo 3º - Acesso a dados e informações

Nos termos da presente política, o acesso aos sistemas e dados da Prime Solutions, S.A, estão condicionados a procedimentos que visam:

i. A autenticação, a autorização, a criptografia, a prevenção e a detecção de intrusão;
ii. A prevenção de fuga de informações;
iii. A realização periódica de testes e auditorias para detecção de vulnerabilidades;
iv. A protecção contra softwares maliciosos;
v. O controlo de acesso e de segmentação da rede de computadores;
vi. A manutenção de cópias de segurança dos dados e das informações;
vii. Controlos específicos para garantir a segurança das informações sensíveis, incluindo de rastreabilidade de informação;
viii. A prestação de informações a clientes e utentes, sobre precauções na utilização de produtos e serviços.

Artigo 4ª – Protecção do ciberespaço

Os procedimentos de implementação da presente política estão implementados respeitando as regras de protecção ambiental, conferindo uma gestão responsável dos controlos e transacções processadas nos servidores, conferindo confiança aos dados processados e a utilização racional e segura dos servidores e backups (de redes locais, internet, redes de comunicações e dados de computação em nuvem).

Artigo 5º - Segurança física e lógica

1. Todas as instalações e equipamentos de suporte ao processamento de informações e dados, nos sistemas informação e tecnologias de suporte encontram-se localizados em áreas seguras, protegidos contra situações de catástrofes naturais e cujo acesso encontra-se condicionado a procedimentos de comunicação prévia e autenticação da entidade.

2. Os critérios de implementação de qualquer tecnologia ou equipamento de suporte estão condicionados a apresentação de um plano de acção ao órgão de gestão, com a descrição detalhada dos objectivos e material ou tecnologia de suporte.

3. Toda a tecnologia ou material de terceiros só poderá ser utilizada/implementada nos sistemas da Prime Solutions, S.A, após a execução de testes de implementação, integridade e aceitação.

Artigo 6º - Controlo de acessos aos sistemas

1. Estão implementados procedimentos de controlo e monitorização dos acessos *on job* e remotos, com base em políticas de encriptação de palavras-passe e definição de privilégios com base nos limites e competências dos colaboradores da Prime Solutions, S.A.

2. O processamento, armazenamento de dados e computação em nuvem é feito com base em políticas de autenticação de acessos.

3. A subcontratação destes serviços fica condicionado a procedimentos de diligencia legal, financeira e operacional.

Artigo 7º - Continuidade de Negócios

1. A gestão dos dados e sistemas informáticos é concebida com vista a gestão da continuidade das operações d Prime Solutions, S.A, em caso de suspensão temporária ou definitiva dos serviços na sede, estando, por isso, implementados procedimentos de redundância e backup de informação, sendo possível continuar e recuperar os dados processados em menos de 24 horas.

2. Estão previstos, dentro da matriz de gestão dos sistemas da Prime Solutions, S.A, a realização de testes a integridade e fiabilidade dos sistemas, com vista a aferir a capacidade de resposta destes.

3. Para a implementação do referido processo, a par dos sistemas de suporte digitais, estão criadas equipas compostas por funcionários chave, capazes de dar continuidade as operações e transacções, incluindo um membro da função de auditoria interna, com o objectivo de auxiliar na salvaguarda dos procedimentos de controlo implementados.

Artigo 8 º Responsabilidades

1. O asseguramento da implementação e monitorização da presente política é da responsabilidade do Departamento da Sistemas de Informação e comunicação, a quem compete assegurar a aquisição dos equipamentos e softwares relevantes a operação da Prime Solutions, S.A, e verificar o estado e a qualidade dos critérios de segurança cibernética.

2. Cabe a função de auditoria interna realizar, dentro do apetite ao risco identificado, auditorias e inspecções aos controlos referentes a política de segurança cibernética e de informação e assegurar, no mínimo:

    - A existência de uma base de dados sobre os riscos identificados e o devido acompanhamento do seu processo de saneamento.
    - A existência de uma base de dados sobre todas as fraudes ocorridas e o processo de saneamento destas.
    - Acompanhamento de todas as situações de violação dos princípios de compliance cibernético e prevenção de fraude, denunciados na Prime Solutions, S.A.
    - Avaliar a compatibilidade entre os princípios do Código de Ética e Conduta Profissional e à presente política.

Artigo 9º - Obrigação de Notificação de Incidentes

No âmbito da presente política, a Prime Solutions, S.A, obriga-se a:

a. Comunicar a **APD (Agência de Protecção de Dados)**, as violações das redes e dos sistemas de informação ou perdas de integridade com impacto significativo no funcionamento das referidas redes e serviços.

b. Comunicar sobre a detecção de incidentes, com intervalos de 4 horas, até à reposição normal dos serviços.

c. Sem prejuízo do dever de sigilo profissional e de livre concorrência, sempre que necessário, a Prime Solutions, S.A, desenvolve iniciativas para a partilha de informações sobre os incidentes relevantes, visando a mitigação do impacto e reforço da resiliência do mercado a ataques cibernéticos.

Artigo 10º- Dúvidas e omissões

1. As regras contidas na presente Política não podem estar em conflito com disposições internas e legislação vigente, nomeadamente a legislação financeira, sobre a protecção de dados e sistemas informáticos, laboral e criminal, sendo que, em caso de dúvida, aplica-se a legislação competente.

2. As dúvidas que surgirem na interpretação e aplicação desta Política serão esclarecidas pela função de *Compliance*.

Artigo 11º- Entrada em vigor

A presente Política entra, imediatamente, em vigor após aprovação e publicação pelo Órgão de Gestão da Prime Solutions, S.A e, sempre que necessário, serão revistos os termos e condições de aplicação da presente política.

Luanda, 30 de Outubro de 2022.

Presidente do Conselho de Administração

Virgílio Mendes