Intervenção do Governador, Dr. Óscar Santos, no Workshop Regional Virtual sobre Risco Cibernético, Afritac West 2, 25 de março de 2021

Banco de Cabo Verde

Avenida Amílcar Cabral • Caixa Postal 101 • Telefone (+238) 2607000 • Fax (+238) 2614447 • Praia – Cabo Verde
www.bcv.cv

Exmo Sr. Director do Centro Afritac West 2,
Exmos Senhores Supervisores Bancários,
Senhores Conferencistas,
Prezados Convidados,
Minhas Senhoras e Meus Senhores,

Muito bom dia a todos!

É com muita satisfação que encerro este importante Workshop Regional Virtual sobre o Risco Cibernético. Muito gostaria de agradecer ao Centro Afritac West 2 por este amável convite e a oportunidade dada aos nossos países de capacitação nas principais áreas de supervisão e regulamentação do setor macroeconómico e financeiro. Em particular gostaria de agradecer os esforços no sentido de apoiar no fortalecimento da estabilidade financeira em Cabo Verde.

As novas tecnologias de informação e comunicação mais do que matéria prima constituem condições essenciais para o crescimento económico e o desenvolvimento dos países. Existe uma dependência cada vez maior das organizações e do sistema financeiro em relação às novas tecnologias de informação. O ambiente económico financeiro é cada vez mais digital possibilitando assim a realização de diversas operações financeiras através de computadores e *smartphones.*

O contexto da pandemia provocada pela Covid-19 veio acentuar ainda mais esta dependência desbravando caminhos para um investimento ainda maior no teletrabalho e no acesso remoto aos sistemas de informação.

Um dos grandes desafios que as nossas economias enfrentam é a inclusão financeira, qual seja das micro-empresas com recurso às novas tecnologias. De notar que nas nossas

economias uma parte substancial é constituída pelas economias informais na qual são praticadas taxas de juros exorbitantes.

A informação é um ativo que, como outros ativos importantes no negócio, tem valor para a organização e se tem valor para a organização consequentemente, necessita de proteção adequada. A segurança da informação está relacionada com a proteção de um conjunto de dados, no sentido de preservar o valor que representa para uma organização.

A transformação digital traz inúmeros benefícios à sociedade ao democratizar o acesso aos serviços financeiros e aumentar a concorrência com reflexo direto no custo das operações.

No entanto, o crescente aumento de ataques cibernéticos, a violação de dados e ataques de negação de serviço, altamente direcionados a instituições financeiras, justificam a preocupação mundial com os riscos cibernéticos.

Definir, alcançar, manter e melhorar a segurança da informação constituem, pois, atividades essenciais para se assegurar o cumprimento da missão dos Bancos Centrais. Estes têm o desafio de proteger os dados institucionais e os dados do consumidor do sistema financeiro.

É facto que o risco cibernético deixou de ser considerado meramente um problema de tecnologias de informação para passar a ser um desafio estratégico do negócio e considerado um risco operacional.
Em Cabo Verde de referir o ataque (*Ransomware*) à Rede Tecnológica Privativa do Estado, no dia 30 de novembro de 2020, que condicionou, temporariamente, vários serviços públicos e privados no país.

Cabo Verde dispõe, desde o dia 29 de janeiro de 2021, de um Regime Jurídico de Cibersegurança (Decreto-lei nº 9/2021 de 29 de janeiro) que visa garantir um elevado nível de segurança das redes e dos sistemas de informação em Cabo Verde.

Trata-se de um diploma que adota as Diretivas C/DIR.1/08/11 da Comunidade Económica dos Estados da África Ocidental (CEDEAO), visando a sua gradual convergência normativa com as comunidades, organizações e demais Estados com os quais Cabo Verde mantém cooperação nesta matéria.

O Banco de Cabo Verde, enquanto um dos pilares do sistema financeiro, monetário e cambial cabo-verdiano tem investido fortemente no desenvolvimento tecnológico enquanto recurso indispensável para o seu crescimento e o cumprimento cabal da sua missão, de forma eficaz e eficiente.
No contexto da pandemia de Covid-19, com a declaração de Estado de Emergência e a imposição de confinamento obrigatório, o sistema financeiro e o próprio Banco Central tiveram que se adaptar rapidamente e preparar os seus sistemas para funcionar em modo contingência.

O Banco Central de Cabo Verde ao nível da segurança da informação tem investido em quatro vertentes: (i) Pessoas, (ii)Tecnologias de informação, (iii) Processos/Controlos e (iv) Estruturas:

Ao nível das pessoas o Banco de Cabo Verde investe sobretudo em campanhas de sensibilização de prevenção e de manuseio/proteção de dados pessoais promovendo uma cultura de cibersegurança em como "a *segurança é uma responsabilidade de todos"*.

No que toca às Tecnologias de Informação procedeu-se à criação de um novo *data center* com um elevado nível de segurança em termos de infraestruturas, a instalação de equipamentos de segurança, a utilização de sistemas *antispam* e antivírus, de

criptografias de dados, a implementação de backups bem como do *desaster recovery site*.

Quanto aos Processos/Controlos o Banco de Cabo Verde tem trabalhado na definição de políticas de segurança da informação, de normas e regulamentos de segurança da informação, de procedimentos, realizado testes de intrusão, auditorias internas e externas assim como a definição e adoção de normas internacionais.

Relativamente às Estruturas estas tem passado pela criação de um serviço de monitorização de sistemas críticos, reestruturação da unidade responsável pelos sistemas e segurança de informação do BCV e o reforço da equipa de TI responsável pela segurança cibernética.

São inúmeros os desafios que o Banco de Cabo Verde enfrenta ao nível da segurança cibernética. São designadamente o alinhamento com as boas práticas internacionais, a definição de política de riscos de segurança da informação, da política específica de segurança cibernética, da política de acesso remoto no âmbito do teletrabalho, cooperação com as diversas entidades nacionais com responsabilidades na segurança da informação bem como o acompanhamento da transformação digital com o intuito de proteger o consumidor final.

Aos riscos cibernéticos estão associados o branqueamento de capitais e o terrorismo. Estes constituem fortes ameaças ao financiamento normal das economias, comércio e pagamentos internacionais.

O risco cibernético é um desafio global, neste quadro temos de trabalhar conjuntamente para o minimizar, tanto quanto possível. A cooperação entre as instituições é de fundamental importância.

Desejamos que este Workshop Regional Virtual sobre Risco Cibernético tenha sido muito proveitoso para as instituições que estão aqui representadas.

Fica assim encerrado este importante Workshop Regional Virtual sobre o Risco Cibernético.

Muito obrigado!

Praia, 25 de março de 2021

Óscar Santos

/Governador do Banco de Cabo Verde/