MATRIZ DE CONSTATAÇÕES E RESPECTIVAS RECOMEMDAÇÔES NO ÂMBITO DA CONFERENCIA NACIONAL DE CIBERSEGURANAÇA

O presente documento sintetiza um conjunto de recomendações com vista a fazer face as principais constatações aferidas no âmbito da Conferencia acima indicada.

Os aspectos críticos que consubstanciam os temas discutidos englobam:

1. Apresentação de ataques cibernéticos e o seu impacto sobre o cidadão e infra-estruturas críticas;
2. Infra-estruturas de suporte aos serviços ao cidadão;
3. Serviços baseado na Internet e o impacto para a vida do cidadão;
4. Os meus dados e a minha privacidade;
5. Novas tecnologias e o incremento do desafio da segurança cibernética;
6. Mecanismos de coordenação e cooperação.
7. Conclusões e Recomendações

		Acções Acordadas	Responsável	Prazo
	As recomendações desta conferencia devem se traduzir em acções concretas com prazos e responsabilidades definidos para permitir melhor seguimento;	.		
Painel 1	Devem ser estabelecidos mecanismos de consciencialização em relação a adopção de práticas seguras no uso da internet; Devem ser tomadas medidas mais céleres para responder aos ataques cibernéticos; Implementar mecanismos que assegurem a continuidade de negócio tendo em conta as mudanças climáticas (olhando como exemplo os ciclones IDAI e kenneth) que já são uma realidade no País; É imperioso encontrar mecanismos de mapeamento e proteção das infraestruturas críticas essenciais para o Estado; Há necessidade de investir mais em segurança quer a nível das Instituições publicas e privadas;			

	É urgente a aprovação da Politica e estratégia Nacional de segurança cibernética para permitir que cada sector elabore a sua estratégia interna de segurança cibernética; A nível das varias instituições devem existir pessoas formadas para lidar com matérias de segurança; As Instituições devem estabelecer CSIRTs que constantemente devem colaborar com o CSIRT do Governo; Os gestores de topo das varias instituições devem ser capacitados sobre matérias ligadas a segurança cibernética, para auxiliarem na tomada de decisão. É importante que os profissionais existentes na área de segurança cooperem mais, criem fóruns de debate regular como forma de criar sinergias para fazer face aos desafios da segurança cibernética. Deve ser feita uma monitoria permanente e a respectiva divulgação dos vários tipos de ataques cibernéticos que estão a ocorrer no país, com recomendações das acções que devem ser levadas a cabo para mitigar os riscos causados por estes ataques.	
Painel 2	-Segurança tem custo e não é baixo, contudo devem ser implementadas soluções menos onerosas, como por exemplo o (SPF, DMARC).	

-Criar mecanismos de consciencializar mais o cidadão em relação aos ataques de Engenharia social, que tem estado a tomar proporções alarmantes.

-A nível dos sectores recomenda-se que haja segregação de funções entre as áreas operacionais (IT) e de segurança de SI.

-Implementar SOCs (Centro de Operacoes de Segurança) a nivel das instituicoes devendo estes assegurar monitoria 24/24h e realizar auditorias regulares de segurança;

Criar politicas de segurança a nível das instituições que abordam matérias de construção de senhas;

Efectuar um desenvolvimento de software seguro e assegurar que a segurança cibernética é implementará de forma holística;

As instituições privadas e publicas devem adoptar boas praticas práticas para garantir a segurança cibernética usando uma abordagem voltada a pessoas, processos e tecnologias;

Necessidade de se aprovarem instrumentos legais que versam sobre esta matéria;

Painel 3	Deve ser implementada de forma effectiva à interoperabilidade de todos os sistemas a nível do governo eletrônico; Os profissionais de segurança precisam definir prioridades e este exercício deve ser feito de forma estruturada; Criar mecanismos de controle em relação a utilização das redes sociais Assegurar que aa nível das instituições do governo sejam usado o domínio @gov.mz para troca de informação de caracter institucional.	
Painel 4	O País deve adoptar uma única linha de actuação em relação a proteção de dados e privacidade; Os pais devem educar e monitorar de forma permanente as crianças na utilização da internet	
Painel 5	Assegurar e implementar mecanismos de cooperação entre os vários sectores evitando a adopção de iniciativas isoladas; Deve se fortificar os mecanismos de cooperação com as varias entidades nacionais e internacionais que tratam de matérias relacionadas a segurança cibernética.	

	Assegurar a adopção a nível da união Africana de regulamentos específicos sobre a matéria de segurança cibernética	
Painel 6		
Painel 7		

Maputo, 14 de Novembro de 2019

O Secretariado