INSTRUTIVO N.º 10/2020

de 29 de Maio

ASSUNTO: SISTEMA FINANCEIRO

- Reporte de Incidentes de Segurança Cibernética

Havendo necessidade de se definir os procedimentos de prestação de informação relativos a quaisquer situações com impacto significativo nos resultados ou capital próprio das Instituições Financeiras, incluindo incidentes de índole operacional, associados à segurança cibernética e à computação em nuvem susceptíveis de afectar a estabilidade do Sistema Financeiro Angolano;

Convindo, igualmente, assegurar e reforçar a fiabilidade das infra-estruturas dos sistemas de informação e da segurança dos dados dos clientes das Instituições Financeiras, conforme estabelecido no Aviso n.º 08/2020, de 02 de Abril;

Nestes termos, ao abrigo das disposições combinadas da alínea j) do artigo 90.º da Lei n.º 12/15, de 17 de Junho – Lei de Bases das Instituições Financeiras e da alínea f) do número 1 do artigo 21.º e do artigo 51.º, ambos da Lei n.º 16/10, de 15 de Julho – Lei do Banco Nacional de Angola.

DETERMINO:

1. Objecto e Âmbito

1.1 O presente Instrutivo estabelece o dever de comunicação de incidentes de segurança cibernética ao Banco Nacional de Angola que sejam classificados como significativos ou muito significativos.

1.2 O presente Instrutivo é aplicável às Instituições Financeiras sob supervisão do Banco Nacional de Angola, adiante abreviadamente designadas por Instituições, nos termos e condições previstos na Lei de Bases das Instituições Financeiras.

2. Âmbito de Incidentes de Segurança Cibernética

2.1 Para efeitos do presente Instrutivo, consideram-se incidentes de segurança cibernética as violações na política de segurança de um sistema de informação de uma Instituição, afectando os pressupostos da sua segurança, dentre as quais destacamos a disponibilidade, integridade e confidencialidade do referido sistema.

2.2 As Instituições referidas no número 1 do presente Instrutivo devem comunicar, em base individual e consolidada, ao Banco Nacional de Angola, todos os incidentes cibernéticos que produzam danos económicos e financeiros, sociais e reputacionais nas entidades incluídas no perímetro de supervisão, independentemente do local onde estas últimas prestam a sua actividade, no prazo de 4h após a detecção do primeiro incidente.

3. Classificação de Incidentes de Segurança Cibernética

3.1 As Instituições devem classificar como significativos ou muito significativos os incidentes de segurança cibernética, usando para o efeito os dados e informações recolhidas no âmbito da avaliação de risco cibernético, o qual engloba também o impacto derivado dos mesmos, sendo que os parâmetros identificados (significativos e muito significativos) devem estar alinhados entre a área de tecnologias de informação e de negócio, visando essencialmente evitar danos económicos e financeiros, sociais e reputacionais decorrentes destes incidentes.

3.2 Sem prejuízo do disposto no subponto anterior, o Banco Nacional de Angola pode, com base na sua avaliação dos incidentes, alterar o nível de risco apresentado pela referida Instituição.

4. Indicações Relativas a Critérios de Materialidade

4.1 Para determinar o número de utilizadores afectados, devem ser considerados todos os clientes, nacionais ou estrangeiros, particulares ou empresas, que possuam uma relação contratual com as Instituições abrangidas pelo presente Instrutivo.

4.2 Para avaliação de incidentes relacionados com a computação em nuvem e servidores, é preciso analisar se as bases de dados centrais e *back-ups* foram comprometidos e que informações constavam em cada uma delas.

4.3 Para o cálculo do potencial impacto económico, devem ser consideradas as perdas globais, directas e indirectas, associadas à ocorrência do incidente de segurança cibernética.

4.4 As perdas globais previstas no subponto anterior devem ser avaliadas em termos absolutos ou, em alternativa, com base na importância relativa para a Instituição.

4.5 Qualquer incidente de segurança cibernética deve ser considerado significativo se resultar em incumprimentos legais ou regulamentares por parte da entidade afectada.

4.6 Qualquer incidente de segurança cibernética com potencial risco sistémico deve ser considerado muito significativo.

5. Canal de Comunicação

5.1 As Instituições devem comunicar ao Banco Nacional de Angola os incidentes classificados como significativos ou muito significativos através do Portal das Instituições Financeiras (PIF).

5.2 Nos casos em que Instituições não tem temporariamente capacidade operacional para assegurar a comunicação do incidente no PIF, ou em casos em que o mesmo esteja indisponível, em consequência do incidente ou por outro motivo de natureza eminentemente técnica (devidamente justificado), o reporte deve ser feito, a título excepcional, através de correio electrónico remetido para o seguinte endereço: reportecibernético@bna.ao.

6. Forma de Comunicação

6.1 As Instituições devem recolher toda a informação possível sobre o incidente e preencher os campos de informação requeridos no reporte, conforme **Anexo** do presente Instrutivo.

6.2 As entidades podem enviar informação adicional que entendam ser relevante para o Banco Nacional de Angola.

6.3 O Banco Nacional de Angola pode em qualquer altura e sempre que lhe se revelar necessário solicitar às instituições informação adicional sobre os incidentes de segurança cibernética reportados.

7. Modelo de Comunicação

7.1 O reporte de incidentes divide-se em três fases: **Inicial**, **Intercalar e Final**, que devem ser preenchidas, de forma incremental e sequencial.

7.2 As Instituições devem submeter o reporte inicial na periodicidade definida no artigo 8.º do Aviso do Aviso n.º 08/2020, de 02 de Abril, sobre Política de Segurança Cibernética e Adopção de Computação em Nuvem. O reporte inicial deve incluir informação com as características gerais do incidente, bem como possíveis consequências do mesmo.

7.3 As Instituições devem submeter um reporte intercalar no prazo de 20 (vinte) dias, após o reporte inicial, preenchendo os campos de informação identificados no modelo de reporte. O reporte intercalar deve conter informação detalhada sobre o tipo de incidente e o seu impacto.

7.4 As Instituições devem submeter um reporte final no prazo de até 45 (quarenta e cinco) dias após o reporte inicial. O reporte final deve reflectir a informação recolhida na investigação interna das causas do incidente, bem como potenciais medidas mitigadoras adoptadas ou previstas para resolver o incidente e evitar a sua recorrência no futuro.

7.5 Na eventualidade do incidente não ficar inteiramente resolvido no prazo de 45 (quarenta e cinco) dias úteis, após o reporte inicial, as Instituições devem ainda assim submeter o reporte final ao Banco Nacional de Angola no prazo estipulado para o efeito.

7.6 Sem prejuízo do subponto anterior, as instituições devem, sempre que o incidente não seja superado depois de 45 (quarenta e cinco) dias, a contar da data do reporte inicial, informar o Banco Nacional de Angola, sobre as razões que levaram a não superação do incidente reportado.

8. Sanções

A violação das disposições constantes do presente Instrutivo é punível nos termos da Lei n.º 12/15, de 17 de Junho - Lei de Bases das Instituições Financeiras.

9. Dúvidas e Omissões

As dúvidas e omissões resultantes da interpretação e aplicação do presente Instrutivo são resolvidas pelo Banco Nacional de Angola.

10. Entrada em vigor

O presente Instrutivo entra em vigor no prazo de 30 (trinta) dias após a sua publicação.

PUBLIQUE-SE.

Luanda, 29 de Maio de 2020.

O GOVERNADOR

JOSÉ DE LIMA MASSANO

ANEXO

Modelo de Reporte

Classificação do Incidente: (significativa/muito significativa)	Data do reporte
Reporte de Incidentes Cibernéticos	
Nome da entidade afectada	
Tipo de entidade afectada	
País da entidade afectada (filiais e sucursais/ escritórios de representação)	
Pessoa de contacto na entidade para actualizações	*E-mail:*
	Tel:
Segunda pessoa de contacto na entidade para actualizações	*E-mail:*
	Tel:
Data de detecção do incidente	
Descrição do Incidente	
Reporte inicial (4horas após incidente) Solicita-se uma descrição geral do incidente	
Reporte intercalar (15 dias após incidente) Solicita-se uma descrição detalhada do incidente Incluir informação (se conhecida e/ou aplicável): - Contexto da detecção de incidente, quem esteve envolvido, o que aconteceu, como o incidente foi detectado - Atacante(s), causa do incidente - Sistemas/áreas afectados e impacto - Canais afectados - Especificar se houve terceiras partes/ fornecedores afectados (nome do fornecedor acfetado, como foi acfetado) e qual o impacto sobre a entidade supervisionada	
Reporte final (máximo 45 dias após incidente) Solicita-se informação actualizada relativamente ao Reporte Intercalar e mais detalhes de: - Vulnerabilidades técnicas exploráveis (indicar número CVE, se conhecido) - Vector de entrada - Escalamento interno/ gestão de crises / acções relevantes tomadas - A investigação (partes externas envolvidas) - Acções de remediação - Controlos de segurança adicionais aplicados como resultado do incidente - Lições aprendidas - Análise da causa raíz - Outras informações relevantes	

ANEXO- Modelo de Reporte (Cont)

Descrição do Incidente								
Tipo de incidente	*Malware*		Engenharia Social		Segurança da Informação		Intrusão/Tentativa de Intrusão	
	Ransomware	☐	*Phishing / *ishing*	☐	*Phishing / *ishing*	☐	*Phishing / *ishing*	☐
	Trojan horse	☐	*Spear phishing*	☐	*Spear phishing*	☐	*Spear phishing*	☐
	Virus/worm	☐	*Pretexting*	☐	*Pretexting*	☐	*Pretexting*	☐
	Mobile malware	☐	Outro	☐	Outro	☐	Outro	☐
	Ataque SAAS	☐	Outro	☐				
	Outro:							
	Informação adicional							
	Malware		Recolha de Informação		Fraude		Intrusão/Tentativa de Intrusão	
	Infeção	☐	*Scan*	☐	Utilização indevida ou não autorizada de recursos	☐	Comprometimento de conta	☐
	Distribuição	☐	*Sniffing*	☐				
	Command & Contro	☐	*Pretexting*	☐	Utilização ilegítima de nome de terceiros	☐		☐
	Indeterminado	☐	Outro	☐			Tentativa de login	
Incidente descoberto por	Segurança TI	☐	Auditor externo	☐	Atacante (aviso)	☐	Empregado interno	☐
	Fornecedor externo	☐	Outro	☐	Auditoria interna	☐	Cliente	☐
	Outro:							
Informação sobre o(s) atacante(s)	Terroristas	☐	*Hacktivistas*	☐	Desconhecidos	☐	*Hackers* (patrocínio de estados)	☐
	Empregados internos	☐	Outros	☐	Outros *hackers*	☐		
	Outro:							
Impacto do incidente (possível múltiplas selecções)	Fuga de informação	☐	Verificou-se a quebra de requisitos legais ou regulatório	☐	Verificou-se alguma cobertura mediática?	☐		
	Fuga de informação relacionada com a instituição?	☐	Se sim, pf indicar		Se sim, pf especifique.			
	Fuga de informação sensível de clientes?	☐						
	Disrupção de serviço crítico?	☐						
	Se sim, horas de disrupção:							
	Fornecedor externo afetado?	☐						
	ATMs afetadas?	☐						
	Fraude em Banca *online*?	☐						
	Houve perdas financeiras diretas ou indirectas?	☐						
	Perdas financeiras diretas em euros							
	Perdas financeiras indiretas estimadas em euros							
	Outros impactos	☐						
	Outro:							

ANEXO – Modelo de Reporte (Cont.)

Serviços e componentes afectados (possível múltiplas selecções)	Estações de trabalho/ clientes (*laptops* , PCs, OSs, *user applications* , etc)	☐	Aplicações cliente/ *software* relacionadas com Banca (vendas, transaccionais, crédito, risco, etc)				
	Redes e telecomunicações (*firewalls, routers, switches, PBX* , etc)	☐	Aplicações empresariais (*SAP, Oracle,* etc)				
	Gestão e armazenamento de dados (*fileservers, databases, data warehouses* , etc)	☐	Plataformas *internet* (*webservers, application servers* , etc)				
			Outros				
	Outro:						
Áreas de negócio afectadas (possível múltiplas selecções)	Finanças Corporativas	☐	Vendas e *trading*	☐	Banca de Retalho	☐	Banca Comercial
	Pagamentos e Contabilidade	☐	Serviços de Agências	☐	Gestão de Ativos	☐	Corretagem de Retalho
	Outros	☐					
	Outro:						
Outros dados relevantes							