PELOURO DE ESTABILIDADE FINANCEIRA
CIRCULAR N.º 01/EFI/2026

Maputo, 14 de Janeiro de 2026

ASSUNTO: MODELO DE REPORTE DE INCIDENTES TECNOLÓGICOS E CIBERNÉTICOS

O Banco de Moçambique estabeleceu, por meio do Aviso n.º 8/GBM/2025, de 9 de Dezembro, as directrizes para o reporte de incidentes tecnológicos e cibernéticos. Nos termos deste Aviso, as instituições de crédito e sociedades financeiras devem reportar os incidentes tecnológicos e cibernéticos, mediante o preenchimento de modelos de reporte a serem definidos por Circular.

Assim, ao abrigo do disposto no n.º 1 do Artigo 5 e alínea b) do artigo 8, do referido Aviso, o Banco de Moçambique determina:

1. As instituições de crédito e sociedades financeiras devem remeter ao Banco de Moçambique o reporte de incidentes tecnológicos e cibernéticos de acordo com o modelo de reporte constante no Anexo I.
2. A relação agregada dos incidentes tecnológicos e cibernéticos deve ser remetida ao Banco de Moçambique, de acordo com o modelo de reporte constante no Anexo II.
3. Os modelos a que se referem os números I e II devem ser remetidos através do Portal BSA (*Banking Supervision Application*) e outros meios indicados pelo Banco de Moçambique.
4. Nos casos em que as instituições de crédito e sociedades financeiras não possuam, temporariamente, capacidade operacional para assegurar a comunicação dos incidentes por via dos meios indicados no número anterior, ou os referidos meios estejam indisponíveis, o reporte deve ser efectuado, a título excepcional, através de correio electrónico: **dsp_riscocibernetico@bancomoc.mz**
5. A presente Circular entra em vigor no dia 9 de Março de 2026.

As dúvidas na interpretação e aplicação da presente Circular devem ser submetidas ao Departamento de Supervisão Prudencial do Banco de Moçambique.

BANCO DE MOÇAMBIQUE
Pelouro da Estabilidade Financeira

Maria Esperança Majimeja
(Administradora)

Anexo I - Modelo de Reporte de Incidentes Tecnológicos e Cibernéticos

Preliminar	☐	**Até 24 horas, contadas do momento da sua ocorrência**
Intermédio	☐	**Até 10 dias úteis, contadas do momento da submissão do relatório preliminar**
Final	☐	**Até 30 dias úteis, após o reporte preliminar**

Identificação do Incidente:

Código da Instituição	
Ano económico	
Data	
Hora de reporte ao BM	

A - Relatório Preliminar	
Detalhes de contacto (1)	
Contacto 1	
Nome:	
Cargo:	
E-mail	
Telefone:	
Contacto 2 (se disponível)	
Nome:	
Cargo:	
E-mail	
Telefone:	
Detalhes do Incidente (2)	
Data da ocorrência	**DD/MM/AAAA**
Hora	**HH:MM**
Tipo de Incidente	☐ Tecnológico ☐ Cibernético
Descrição do Incidente	
B - Relatório Intermédio	
(1) Informações sobre a origem	☐ Trabalhador ☐ Provedores de serviço ☐ *Hackers* ☐ Utente do serviço ☐ Desconhecido Outros. Especificar: _____

(2) Existe relação com outro incidente reportado anteriormente?	☐ Sim	Fornecer detalhes: Data: Hora:
	☐ Não	
(3) Componentes afectados	☐ Estações de trabalho (*laptops*, PCs, dispositivos móveis) ☐ Sistemas Operativos ☐ Sistemas principais (sistemas informáticos que suportam as áreas de negócio) ☐ Sistemas periféricos (sistemas informáticos que suportam as áreas de controlo e de suporte) ☐ Canais digitais (*internet banking*, aplicações mobile) ☐ Sistemas de gestão de dados e de armazenamento (*file servers*, bases de dados, *data warehouse*) ☐ Aplicações de escritório ☐ Correio electrónico ☐ Redes e telecomunicações (*switches, routers, firewalls,* PBX, VoIp, *call center*) ☐ Servidores ☐ Componentes de *middleware* (processadores, equipamentos de camadas intermédias) ☐ Outros. Especificar: _____	
(4) Áreas Afectadas		
(4.1) Áreas de negócio afectadas	☐ Finanças/contabilidade ☐ Área comercial (corporativa e retalho) ☐ Mercados financeiros (mercado monetário interbancário, cambial e *forex*) ☐ Canais digitais/electrónicos (transacções com cartões, *Internet Banking*, *Mobile banking*, carteiras móveis) ☐ Gestão de operações (de balcão, estrangeiro, gestão de contas de clientes, operações de compensação e liquidação) ☐ Tesouraria ☐ Gestão de crédito (originação, análise, administração e recuperação/monitoramento de crédito) ☐ Outros. Especificar: _____	
(4.2) Áreas de controlo afectadas	☐ Risco ☐ *Compliance* ☐ Auditoria interna ☐ Controlo interno ☐ Segurança de Sistemas/Cibernética ☐ Gestão de fraudes ☐ Outros. Especificar:_____	
(4.3) Áreas de suporte afectadas	☐ Recursos Humanos ☐ Tecnologia de Informação ☐ Aquisição de bens e serviços ☐ Jurídico/legal ☐ Gestão de reclamações de clientes ☐ *Marketing* ☐ Outros. Especificar:_____	

(5) Classificação do incidente quanto à natureza	**INCIDENTE TECNOLÓGICO**
	Problemas com sistemas ☐ Erro/falha de configuração ☐ Indisponibilidade de sistemas ☐ Lentidão de sistemas ☐ Erros/Falhas na actualização de versões ☐ Outros. Especificar:_____
	Falhas de equipamento ☐Configuração incorrecta ☐ Obsolescência ☐ Dano ou quebra física de equipamento ☐ Sobrecarga ☐ *Firmware* não actualizado ☐ Outros. Especificar:_____
	Falhas/Interrupção da infraestrutura de redes de comunicações ☐ Erros/falhas de equipamentos de Rede ☐ Problemas com cabos e conexões físicas ☐ Falhas em ligações de internet ou provedor de serviço ☐ Congestionamento e sobrecarga de rede ☐ Problemas de configuração de rede ☐ Falhas em equipamentos de comunicação wireless ☐ Falhas em sistemas de alimentação e energia ☐ Problemas de latência e perda de pacotes ☐ Outros. Especificar:_____
	INCIDENTE CIBERNÉTICO
	Conteúdo abusivo ☐ *SPAM* ☐ Crime de ódio ☐ Pornografia ☐ Outros. Especificar:_____
	Código malicioso ☐ *Worm* ☐ *Trojan* ☐ *Spyware* ☐ *Dialler* ☐ *Rootkit* ☐ Outros. Especificar:_____
	Recolha de informações ☐ *Scanning* ☐ *Sniffing* ☐ Engenharia social ☐ Outros. Especificar:_____

	Tentativa de intrusão ☐ Exploração de vulnerabilidades conhecidas ☐ Tentativa de acesso com violação de credenciais ☐ Ataque desconhecido ☐ Outros. Especificar:_____
	Intrusão ☐ Comprometimento de conta privilegiada ☐ Comprometimento de uma conta sem privilégios ☐ Comprometimento de aplicações ☐ Outros. Especificar:_____
	Disponibilidade ☐ DoS (*Denial-of-Service*) ☐ DDoS (*Distributed Denial-of-Service*) ☐ Má configuração ☐ Sabotagem ☐ Interrupções ☐ Outros. Especificar:_____
	Comprometimento de informações ☐ Acesso não autorizado a informações ☐ Alteração não autorizada de informações ☐ Perda de dados ☐ Outros. Especificar:_____
	Fraude ☐ Utilização não autorizada de recursos ☐ Direitos de autor ☐ Falsificação de identidade ☐ *Phishing* ☐ Outros. Especificar:_____
	APT (*Advanced Penetration Threat*)
	Outros (por especificar)
(6) Classificação do incidente quanto a gravidade	☐ Crítico ☐ Alto ☐ Médio
(7) Que acções ou respostas foram tomadas pela instituição	
(8) Incidente identificado por:	☐ Segurança cibernética ou de SI ☐ Tecnologias de Informação ☐ Auditoria interna ☐ Auditoria externa ☐ Prestador de serviços ☐ Cliente ☐ Trabalhador ☐ Outros. Especificar: _____

<table>
<tr><th colspan="4">(9) Impacto do incidente</th></tr>
<tr><td rowspan="4">(9.1) Impacto na reputação</td><td rowspan="2">Nível de visibilidade</td><td colspan="2">☐ Nacional</td></tr>
<tr><td colspan="2">☐ Internacional</td></tr>
<tr><td rowspan="2">Houve alguma cobertura a nível dos meios de comunicação?</td><td colspan="2">☐ Sim
☐ Não</td></tr>
<tr><td colspan="2">Se sim especifique:
_____</td></tr>
<tr><td>Nível de reclamações dos clientes face ao produto ou serviços providos pelo banco</td><td colspan="2">☐ Recorrentes
☐ Significativas
☐ Pontuais
☐ Esporádicas e isoladas</td></tr>
<tr><td>(9.2) Impacto Financeiro</td><td colspan="3">Potenciais prejuízos financeiros:

☐ >=0,50% dos fundos próprios de base Tier1
☐ 0,20 % <= dos fundos próprios de base Tier1 < 0,50%
☐ 0,10 % <= dos fundos próprios de base Tier1 < 0,20%
☐ < 0,10% dos fundos próprios de base Tier1</td></tr>
<tr><td></td><td colspan="3">Outros. Especificar: _____</td></tr>
<tr><td>(9.3) Impacto Operacional</td><td colspan="3">☐ Interrupção de serviços críticos que excedam o SLA e/ou RTO instituídos

Especificar o(s) serviço(s) crítico(s): _____
Indique as horas de interrupção por serviço: _____</td></tr>
<tr><td></td><td colspan="3">☐ Clientes afectados (em termos percentuais ou absolutos). Número de Clientes : _____</td></tr>
<tr><td></td><td colspan="3">A resolução/mitigação do incidente implica:
☐ A activação do Plano de Continuidade de Negócio (PCN);
☐ Alocação de recursos externos
☐ Alocação de recursos internos
☐ Outros. Especifique: _____</td></tr>
<tr><td>(10) Provedores de serviços originário do incidente</td><td colspan="3">☐ Não</td></tr>
<tr><td></td><td>☐ Sim</td><td colspan="2">Identificação do provedor</td></tr>
<tr><td></td><td></td><td colspan="2"></td></tr>
</table>

<table>
<tr><td rowspan="2">(11) O incidente foi resolvido?</td><td>☐ Sim</td><td>Medidas tomadas para resolução do incidente</td></tr>
<tr><td>☐ Não</td><td>Acções de remediação propostas
<table><tr><th>Acção de Remediação</th></tr><tr><td></td></tr><tr><td></td></tr><tr><td></td></tr><tr><td></td></tr></table></td></tr>
</table>

C - Relatório Final	
Investigação e resolução do incidente	
1. Ordem sequencial dos eventos	
(1.1) Duração da interrupção	**HH:MM**
(1.2) Descrição da origem	
(1.3) Qual foi o vector de entrada do incidente?	☐ Agente interno (colaboradores de instituição) ☐ Agente externo (provedores de serviços) ☐ Desastres naturais ☐ Corte ou interrupção de fornecimento de energia eléctrica ☐ Corte ou interrupção de serviços de telecomunicações ☐ Equipamentos da infraestrutura tecnológica ☐ Rede de *Internet* ☐ Mensagem instantânea ☐ Telefone ☐ Competências administrativas ☐ *E-mail* ☐ Dispositivos não autorizados ☐ Dispositivos perdidos/roubados ☐ Redes sociais ☐ Vulnerabilidades de segurança ☐ *Phishing* ou *pop-ups* em formulários da *Web* ☐ Engenharia social ☐ Ameaças internas mal-intencionadas ☐ *Spoofing* ☐ Ataques baseados em identidade ☐ Ataques de injecção de código ☐ Outro (por favor, especifique) _____
(1.4) Vulnerabilidades /fraquezas expostas	☐ Equipamento obsoleto ☐ *Software* não actualizado (*firmware* e aplicações) ☐ Gestão inadequada de *patches*☐ Gestão inadequada de contas previlegiadas ☐ Protecção inadequada de e-mail/navegador da *web* ☐ Defesas inadequadas contra *malware* ☐ Gestão inadequada de acessos ☐ Configurações de segurança inadequadas de *hardware* (dispositivos terminais, *laptops*, estações de trabalho, servidores) ☐ Configurações de segurança inadequadas para *software* ☐ Configuração inadequada do perimetro de segurança ☐ Controlo inadequado de portas, protocolos e serviços de rede ☐ *Backup* inadequado de sistemas ou arquivos ☐ Dispositivos de rede não seguros (*firewalls*, roteadores, *switches*) ☐ Controlos de segurança de *software* de aplicativos inadequados (aplicativos baseados na *web* e outros) ☐ Defesa DDoS inadequada ☐ Testes de penetração e de segurança inadequados ☐ Segmentação de rede inadequada ☐ Falta de conscientização e/ou conformidade da equipa ☐ Manutenção e monitoramento inadequados de *logs*

	☐ Falta de pessoal ☐ Criptografia fraca Outros. Especificar: _____	
(1.5) Incidente foi escalado internamente para a gestão de topo, ao nível de grupo, para açções fora dos procedimentos habituais?	☐ Não	
	☐ Sim	A quem? (incluir também o papel na estrutura de governação, quando aplicável)
(1.6) Partes interessadas informadas ou envolvidas	☐ Não	
	☐ Sim	Como foram envolvidos ou informados?
(1.7) Medidas de escalonamento tomadas, incluindo aprovações solicitadas sobre medidas provisórias para mitigar o evento e razões para tomar tais medidas		
(1.8) A ocorrência obrigou a activação de procedimentos de gestão de crise	☐ Não	
	☐ Sim	☐ Planos de resposta e gestão de incidentes cibernéticos, tendo em conta o previsto nas Directrizes de Gestão do Risco e Resiliência Cibernética, aprovadas pelo Aviso n.º 2/GBM/2024, de 15 de Março
		☐ Seguros ou outros instrumentos similares de cobertura de perdas relacionadas com o incidente
		☐ Planos de emergência
		☐ Outros processos ou módulos de crise relevantes da instituição: _____
(1.9) Quem está a liderar a investigação do incidente?	☐ A instituição	
	☐ Provedor do serviço	
	☐ Autoridades policiais ou outras agências de segurança	
	☐ Se outro especificar: _____	
(1.10) Quem está liderar as acções de remediação	☐ A instituição	
	☐ Provedor do serviço	
	☐ Se outro especificar:_____	
(1.11) Factores que causaram o problema/ Razões para ocorrer, causa e efeitos do incidente		
(1.12) O plano de acção definido para a resolução do	☐ Sim	

<table>
<tr><td>incidente foi cumprido na totalidade</td><td>☐ Não</td><td>Se não, indique as razões</td></tr>
<tr><td rowspan="2">(1.13) Acções correctivas tomadas para evitar ocorrências futuras de tipos semelhantes de incidentes</td><td colspan="2">☐ Não</td></tr>
<tr><td>☐ Sim</td><td>Etapas identificados ou a serem tomadas para resolver o incidente a longo prazo</td></tr>
<tr><td colspan="3">(2) Avaliação final e remediação:</td></tr>
<tr><td>(2.1) Perdas financeiras directas e indirectas em meticais</td><td colspan="2"></td></tr>
<tr><td>(2.2) Conclusão sobre causa</td><td colspan="2"></td></tr>
<tr><td>(2.3) Resumo de incidentes semelhantes causados pela mesma causa raiz nos últimos 12 meses</td><td colspan="2"></td></tr>
<tr><td>(2.4) Outras informações complementares</td><td colspan="2"></td></tr>
<tr><td rowspan="2">(2.5) Houve notificação ao cliente/anúncio público/relatório a outros órgãos reguladores relevantes sobre a resolução do incidente</td><td colspan="2">☐ Não</td></tr>
<tr><td>☐ Sim</td><td>Descrição do mecanismo adoptado para a comunicação do incidente ao cliente/anúncio público/relatório a outros órgãos reguladores</td></tr>
<tr><td rowspan="2">(2.6) O incidente foi resolvido?</td><td>☐ Sim</td><td>Indique a data de resolução</td></tr>
<tr><td>☐ Não</td><td>Remeter ao Banco um plano de acções com propostas para a resolução do incidente e respectivos prazos para acompanhamento

<table>
<tr><th>Acção de Remediação</th><th>Prazo</th><th>Status</th><th>Observações</th></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>
</td></tr>
</table>

Anexo II – Modelo de Reporte de Incidentes Tecnológicos e Cibernéticos Agregado

I. INFORMAÇÃO ESTATÍSTICA (QUANTITATIVA)

Código da Instituição	
Ano económico	
Data	
Hora de reporte ao BM	

(1) Total de incidentes reportados pela instituição [ ]

(2) Classificação do Incidente		(3) Vulnerabilidade exposta	(4) Frequência dos incidentes	(5) ID dos Incidentes reportados	(6) Vector de Entrada	(7) Componentes afectadas	(8) Serviços afectados (área de suporte, controlo ou de negócio)	(9) N° Transacções comprometidas	(10) N° de utilizadores afectados	(11) Estado (Resolvido/ Em processo de resolução/ Não Iniciado)
(2.1) Quanto a natureza	(2.2) Quanto a gravidade									
<Exemplo de preenchimento: Spam>	*<alto>*	*<criptografia fraca>*	*<2>*	*<dim01>*	*<rede de internet>*	*SO*	*IT*	*<10>*	*<1000>*	*<resolvido>*
				<dim02>	*<mensagem instantânea>*	*sistema principal*	*mercados*	*<5>*	*<500>*	*<em processo de Resolução>*

II. ANÁLISE DO IMPACTO DOS INCIDENTES REPORTADOS NO PERÍODO

<Coloque a descrição global do impacto dos incidentes com base na tabela que se segue>

(12) Reputacional	
(13) Financeiro	
(14) Operacional	

III. INFORMAÇÕES ADICIONAIS

(15) Outras informações consideradas relevantes:	

Declaramos que a informação contida no Anexo II – Modelo de Reporte de Incidentes Cibernéticos Agregado está de acordo com o registo de incidentes cibernéticos que ocorreram na instituição no período reportado.

Assinatura do membro do Conselho de Administração

_____

Assinatura do responsável

_____

<Local>, aos *<Data>*

1. NOTAS EXPLICATIVAS AO MODELO DE REPORTE DE INCIDENTES CIBERNÉTICOS

A. Relatório Preliminar

Coluna	Descrição	Tipo de dados
(1)	Detalhes dos contactos dos responsáveis pela informação	Texto
(2)	Detalhe do incidente	Texto

B. Relatório Intermédio

Coluna	Descrição	Tipo de dados
(1)	Indicação da origem do incidente	Texto
(2)	Indicação da relação do incidente reportado com outros incidentes	Texto
(3)	Descrição do incidente quanto aos componentes afectados	Texto
(4)	Indicação das áreas afectadas (de negócio, de controlo e de suporte)	Texto
(5)	Classificação do incidente quanto a natureza nos termos do anexo II do Aviso de reporte de incidentes	Texto
(6)	Classificação do incidente quanto a gravidade nos termos do anexo I do Aviso de reporte de incidentes	Texto
(7)	Descrição das acções tomadas para a resolução do incidente	Texto
(8)	Indicação do mecanismo usado para a identificação do incidente	Texto
(9)	Descrição do impacto do incidente a nível reputacional, financeiro e operacional	Alfanumérico (Texto/ Número)
(10)	Indicação da origem do incidente e do provedor de serviço afectado	Texto
(11)	Indicação do estado do incidente tendo em conta o nível e o tempo de resolução do mesmo	Texto

C. Relatório Final

Coluna	Descrição	Tipo de dados
(1)	Descrição detalhada das investigações efectuadas tendo em conta a origem, vulnerabilidades e as acções tomadas para a sua resolução	
(1.1)	Indicação do tempo de duração do incidente em horas	Número inteiro
(1.2)	Descrição detalhada do invasor que esteja na origem do incidente	Texto
(1.3)	Indicação dos mecanismos usados na invasão	Texto
(1.4)	Indicação das fraquezas/vulnerabilidades que o sistema esteve exposto	Texto
(1.5)	Descrição do nível de escalonamento na gestão do incidente	Texto
(1.6)	Indicação dos intervenientes envolvidos na resolução do incidente	Texto
(1.7)	Indicação das medidas tomadas tendo em conta os níveis de aprovação	Texto
(1.8)	Descrição dos procedimentos de gestão de crise activados para a mitigação do incidente	Texto
(1.9)	Indicação da parte interessada responsável pela investigação do incidente	Texto
(1.10)	Indicação da parte interessada responsável pela remediação do incidente	Texto
(1.11)	Descrição da causa do incidente	Texto
(1.12)	Indicação do nível de cumprimento do plano de acção na resolução do incidente	Texto
(1.13)	Descrição das acções correctivas implementadas para que o incidente não se repita	Texto
(2)	Descrição detalhada da natureza do incidente, impactos económicos, lições aprendidas	
(2.1)	Montante de perdas financeiras directas e indirectas decorrentes da ocorrência de incidentes	Numérico
(2.2)	Descrição detalhada sobre a origem do incidente	Texto
(2.3)	Descrição dos incidentes com a mesma causa raiz ocorridos nos últimos 12 meses	Texto
(2.4)	Descrição de Outras informações consideradas relevantes não captadas nos números anteriores	Texto
(2.5)	Descrição do tipo de notificação efectuada após a resolução do incidente	Texto
(2.6)	Descrição do estado do incidente	

2. NOTAS EXPLICATIVAS AO MODELO DE REPORTE DE INCIDENTES CIBERNÉTICOS AGREGADO

I. INFORMAÇÃO ESTATÍSTICA (QUANTITATIVA)

Coluna	Descrição	Tipo de dados
(1)	Indicação do nº de incidentes reportados no período em referência	Número inteiro
(2.1)	Classificar o incidente quanto a natureza nos termos do anexo II do Aviso de reporte de incidentes	Texto
(2.2)	Classificar o incidente quanto a gravidade nos termos do anexo I do Aviso de reporte de incidentes	Texto
(3)	Indicação das fraquezas/ vulnerabilidades que o sistema esteve exposto	Texto
(4)	Indicação do número de vezes que o incidente ocorreu	Número inteiro
(5)	Indicação do número de identificação do incidente reportado	Número inteiro
(6)	Indicação do mecanismo utilizado pelo invasor	Texto
(7)	Indicação dos componentes e sistemas afectados	Texto
(8)	Indicação dos serviços afectados, área de negócio, suporte e controle afectada	Texto
(9)	Indicação do número total de transacções afectadas pelo incidente	Número inteiro
(10)	Indicação do número total de utilizadores afectados pelo incidente	Número inteiro
(11)	Indicação do estado do incidente tendo em conta o nível de resolução do mesmo.	Texto

II. ANÁLISE DO IMPACTO DOS INCIDENTES REPORTADOS NO PERÍODO

Coluna	Descrição	Tipo de dados
(12)	Descrição da magnitude do impacto agregado (quer a nível nacional ou internacional) e do nível de divulgação nos meios de comunicação dos incidentes ocorridos no período	Texto
(13)	Montante total de perdas financeiras directas e indirectas decorrentes da ocorrência de incidentes	Número
(14)	Indicação do número total de horas de indisponibilidade de serviços	Número

III. INFORMAÇÕES ADICIONAIS

Coluna	Descrição	Tipo de dados
(15)	Descrição de outras informações consideradas relevantes não captadas nos números anteriores	Texto