



# BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRESA NACIONAL DE MOÇAMBIQUE, E. P.

## AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

## SUMÁRIO

Banco de Moçambique:

**Aviso n.º 8/GBM/2025:**

Estabelece as directrizes para o reporte de incidentes tecnológicos e cibernéticos.

**Aviso n.º 9/GBM/2025:**

Estabelece limites de pagamentos sobre o exterior efectuados através de cartões bancários.

## BANCO DE MOÇAMBIQUE

**Aviso n.º 8/GBM/2025**

de 20 de Novembro

A relevância da resiliência tecnológica e cibernética no sector financeiro nacional tem-se tornado cada vez mais significativa, o que denota a necessidade de garantir a detecção, comunicação, mitigação e recuperação atempada dos incidentes que possam afectar a confiança dos consumidores, a integridade dos serviços e a estabilidade do sistema financeiro.

Nestes termos, o Banco de Moçambique, no uso das competências que lhe são conferidas pela alínea *d*) do n.º 2 do artigo 37 da Lei n.º 1/92, de 3 de Janeiro, Lei Orgânica do Banco de Moçambique, determina:

### CAPÍTULO I

#### Disposições Gerais

ARTIGO 1

**Objecto**

O presente Aviso estabelece as directrizes para o reporte de incidentes tecnológicos e cibernéticos.

ARTIGO 2

**Âmbito**

O presente Aviso aplica-se às instituições de crédito e sociedades financeiras, doravante designadas por “instituições”.

ARTIGO 3

#### Definições

Os termos e expressões usados no presente Aviso são definidos no Glossário, Anexo 1, que é dele parte integrante.

### CAPÍTULO II

#### Classificação e Reporte dos Incidentes

ARTIGO 4

##### Classificação dos incidentes

- Os incidentes tecnológicos e cibernéticos podem ser classificados quanto à natureza ou gravidade.
- As instituições devem considerar a taxonomia apresentada no Anexo 2 do presente Aviso para a classificação da natureza dos incidentes.
- As instituições devem classificar e reportar os incidentes tecnológicos e cibernéticos, que abrangem eventos externos e internos, provocados ou acidentais, de acordo com os níveis de gravidade descritos no Anexo 3 do presente Aviso.

ARTIGO 5

##### Modelo de reporte

- As instituições devem reportar os incidentes de nível crítico, alto e médio, mediante o preenchimento do modelo de reporte de incidentes, a ser aprovado por Circular.
- Sem prejuízo do estabelecido no número anterior, os incidentes de nível baixo devem ser devidamente documentados e disponíveis para consulta.

ARTIGO 6

##### Prazo de reporte

- As instituições devem reportar os incidentes, de forma incremental, nos seguintes prazos:
  - Reporte Preliminar: vinte e quatro horas, a contar do momento da sua ocorrência;
  - Reporte Intermédio: dez dias úteis, a contar da data de submissão do reporte preliminar; e
  - Reporte Final: até trinta dias úteis, a contar da data de submissão do reporte intermédio.
- Caso o incidente não seja resolvido no prazo estabelecido na alínea *c*) do número anterior, as instituições devem submeter ao Banco de Moçambique, no mesmo prazo, o relatório final e um plano de acção contendo as medidas de mitigação adoptadas ou previstas para resolver o incidente e evitar a sua recorrência.

3. Caso a instituição resolva o incidente num período inferior a vinte e quatro horas, deve submeter:

- a) O relatório preliminar conforme previsto na alínea a) do número 1 do presente artigo; e
- b) Os relatórios intermédio e final no prazo de cinco dias.

#### ARTIGO 7

##### Conteúdo dos reportes

Os reportes devem conter:

- a) Relatório Preliminar: informação de carácter geral, descrevendo as características essenciais do incidente e o seu provável impacto, seguindo o modelo aprovado pelo Banco de Moçambique.
- b) Relatório Intermédio: descrição detalhada do incidente e o seu impacto, devendo ser actualizado sempre que a instituição tiver novas informações relevantes ou alterações significativas; e
- c) Relatório Final: a informação que actualiza o relatório intermédio, acrescida de detalhes sobre a análise da causa raiz do incidente, o resultado da investigação interna, as acções de remediação tomadas ou previstas e as lições aprendidas.

#### ARTIGO 8

##### Reporte agregado

As instituições devem remeter, trimestralmente, até ao dia quinze do mês seguinte ao trimestre a que respeita, a informação contendo a relação dos incidentes ocorridos, devendo, para o efeito, juntar:

- a) A carta de remessa, devidamente assinada por um membro do Conselho de Administração e pelo executivo sénior responsável pela gestão dos incidentes; e
- b) A informação agregada dos incidentes reportados dentro do período considerado, conforme Modelo aprovado por Circular.

#### ARTIGO 9

##### Preservação de informação e dever de colaboração

1. As instituições devem preservar os dados e evidências relacionadas com a ocorrência dos incidentes reportados, por um período mínimo de 10 anos.
2. As instituições devem, igualmente, colaborar com as autoridades reguladoras e de segurança, no âmbito da investigação dos incidentes reportados.
3. Sem prejuízo do disposto nos números anteriores, as instituições devem salvaguardar a observância do dever segredo bancário, a que estão legalmente adstritas.

### CAPÍTULO III

#### Disposições Finais

#### ARTIGO 10

##### Regime Sancionatório

O incumprimento do previsto no presente Aviso constitui contravenção punível nos termos da Lei n.º 20/2020, de 31 de Dezembro. Lei das Instituições de Crédito e Sociedades Financeiras.

#### ARTIGO 11

##### Entrada em vigor

O presente Aviso entra em vigor noventa dias a contar da data da sua publicação.

#### ARTIGO 12

##### Esclarecimento de dúvidas

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

Maputo, 20 de Novembro de 2025. — O Governador, *Rogério Lucas Zandamela*.

### Anexo 1

#### Glossário

##### A

**Activos Críticos** – recursos ou sistemas essenciais para a continuidade das operações de uma instituição, cujo seu comprometimento ou falha tem um impacto significativo nos serviços prestados, na segurança de dados e na reputação institucional.

##### C

**Código Malicioso** – *firmware* ou *software* intencionalmente incluído ou inserido em um sistema para fins prejudiciais.

##### D

**Dialler** – tipo específico de *spyware*, que tem como função gerar ligações para um determinado número de telefone uma vez instalados no computador ou rede do utilizador.

##### E

**Evento** – ocorrência observável num sistema de informação ou rede.

##### I

**Incidente Cibernético** – ocorrência que coloque em risco a integridade, confidencialidade ou disponibilidade da informação, ou constitua uma violação ou ameaça iminente de violação da lei, das políticas de segurança de informação, procedimentos de segurança ou políticas de uso aceitáveis.

**Incidente Tecnológico** – ocorrência que resulta na falha, interrupção ou mau funcionamento de sistemas informáticos, equipamentos ou infraestrutura de redes de comunicações.

##### P

**Proxy** – *software* que recebe pacotes de rede de um cliente e os envia em nome do cliente para o destino desejado.

##### S

**Scanning** – processo de varredura de sistemas, redes ou dispositivos em busca de vulnerabilidades a serem exploradas.

**Sistema Periférico** – sistema informático que não é essencial para as operações principais das instituições, sendo este importante para o negócio, mas não crítico para a sua capacidade de funcionar e servir ao cliente, permitindo que as instituições desempenhem funções como *marketing* e vendas, gestão de recursos humanos, orçamento e colaboração, entre outras.

**Sistema Principal (core)** – todo aquele sistema informático que é essencial para as operações da instituição e que em caso de falha ou interrupção têm um impacto significativo no negócio.

Estes são baseados em quaisquer componentes tecnológicos (*software*, *hardware*, base de dados, processos, aplicações, entre outros) para a execução de funções como gestão de operações financeiras, gestão de cartões bancários, canais digitais e gestão de transações em mercados financeiros.

*Spyware* – *software* que é instalado secretamente num sistema de informação para recolher informações sobre indivíduos ou organizações sem o seu conhecimento.

#### R

**Recovery Time Objectives (RTO)** – tempo aceitável em que um sistema pode ficar indisponível após um desastre.

**Rootkit** – *software* malicioso que permite o acesso privilegiado a áreas de um computador, corrompendo o sistema operativo ou outras aplicações, ocultando a sua presença.

**Ransomware** – *software* que infecta um computador, de modo que o utilizador não possa aceder aos dados armazenados, sendo que a reposição do acesso aos ficheiros bloqueados é condicionada ao pagamento de um valor de resgate.

#### W

**Worm** – programa que tem a propriedade de criar réplicas de si próprio na memória de um computador, assim como a de se propagar de um computador para outro através da rede.

**Anexo 2**  
Taxonomia de Incidentes Quanto a Natureza

Categoria	Classificação	Tipo de Incidente	Descrição do incidente
Incidente Tecnológico	Problemas com sistemas	Erro/falha de configuração	Erros de compatibilidade ou configuração entre sistemas ou de códigos fonte.
		Indisponibilidade de sistemas	Parametrização incorrecta de sistemas ou equipamentos, falhas de equipamentos, ataques cibernéticos, interrupção de redes, manutenção de sistemas, desastres naturais, problemas de alimentação eléctrica e climatização.
		Lentidão de sistemas	Sobrecarga de recursos, aumento do volume transaccional, conexão de rede lenta, aplicações mal optimizadas, concorrência excessiva, fragmentação da base de dados.
		Erros/Falhas na actualização de versões	Incompatibilidade de <i>patches</i> , ambientes de teste inadequados, erro humano, problemas de rede, políticas de segurança rigorosas, interrupções durante a actualização e falta de planeamento e agendamento.
		Outros	Qualquer incidente que não se enquadra em nenhuma das categorias anteriores.
		Configuração incorrecta	Parametrizações inadequadas de equipamentos.
	Obsolescência	Equipamento obsoleto e fora do período de suporte.	

Incidente Tecnológico (cont.)	Falhas de equipamento	Dano ou quebra física de equipamento.	Quebra física de servidores, terminais, dispositivos móveis e equipamentos rede causados por defeitos de fabrico.
		Sobrecarga	Equipamento a funcionar acima das suas capacidades por um período extenso resultante de dimensionamento incorrecto.
		<i>Firmware</i> não actualizado	Falta de actualização do <i>software</i> embutido em <i>hardware</i> .
	Falhas/Interrupção da infraestrutura de redes de comunicações	Outros	Qualquer incidente que não se enquadra em nenhuma das categorias anteriores.
		Erros/falhas de equipamentos de Rede	Falha em <i>switches</i> , roteadores, <i>firewalls</i> e equipamentos de Segurança de Rede, IDS (sistemas de detecção de intrusão) e IPS (sistemas de prevenção de intrusão).
		Problemas com cabos e conexões físicas	Desconexão ou dano de cabos e problemas em pontos de conexão.
		Falhas em ligações de <i>internet</i> ou provedor de serviço	Interrupção do serviço de <i>internet</i> e problemas em conexões de <i>Backup</i> .
		Congestionamento e sobrecarga de rede	Alta utilização de largura de banda e ataques de DDoS (Distributed Denial of Service).
		Problemas de configuração de rede	Configuração incorreta de roteadores e <i>switches</i> e configurações de DNS e DHCP.
		Falhas em equipamentos de comunicação <i>wireless</i>	Problemas em Pontos de Acesso <i>Wi-Fi</i> e interferência de Sinais.
Falhas em sistemas de alimentação e energia	Quedas de energia e picos de tensão.		

		Problemas de latência e perda de pacotes	Alta latência e perda de pacotes.
		Outros	Qualquer incidente que não se enquadra em nenhuma das categorias anteriores.
	Conteúdo abusivo	<i>Spam</i>	Correio electrónico em massa não solicitado. O destinatário do conteúdo não deu uma autorização válida para receber uma mensagem em massa.
	Conteúdo abusivo (cont)	Crimes de ódio, crimes contra a liberdade ou a honra	Conteúdo difamatório ou discriminatório ( <i>cyberbullying</i> , racismo, ameaças a uma pessoa ou dirigidas a grupos, entre outros).
		Pornografia infantil, conteúdos sexuais ou violentos	Material que apresente visualmente conteúdos relacionados com pornografia infantil, apologia da violência, entre outros.
		<i>Worm</i>	<i>Software</i> que é intencionalmente incluído ou inserido num sistema com finalidade prejudicial. Normalmente, é necessária uma interacção do utilizador para activar o código.
		<i>Trojan</i>	
		<i>Spyware</i>	
		<i>Dialler</i>	
		<i>Rootkit</i>	
		<i>Scanning</i>	Ataques que enviam pedidos a um sistema para descobrir pontos fracos. Isto inclui também algum tipo de processos de teste para recolher informações sobre <i>hosts</i> , serviços e contas.
	Recolha de informações	<i>Sniffing</i>	Observação e registo do tráfego da rede (escutas telefónicas).
Incidente Cibernético			

	Engenharia social	Técnicas utilizadas para obter informações confidenciais através de ações que enganam ou exploram a confiança das pessoas.
	Exploração de vulnerabilidades conhecidas	Uma tentativa de comprometer um sistema ou de perturbar qualquer serviço através da exploração de vulnerabilidades.
Tentativa de intrusão	Exploração de vulnerabilidades desconhecidas (Ataque de dia zero)	Tentativas de exploração de uma vulnerabilidade desconhecida num <i>hardware</i> , <i>software</i> ou <i>firmware</i> , para a qual ainda não foi emitida a correção, comprometendo a segurança antes de qualquer mitigação possível.
	Tentativa de acesso com violação de credenciais	Várias tentativas de violação de credenciais. Por exemplo, tentativas de quebra de palavra-passe, ataque de força bruta.
Intrusão	Ataque desconhecido	Tentativa de utilizar uma exploração desconhecida.
	Comprometimento de conta privilegiada	Comprometimento de um sistema em que o atacante adquiriu privilégios elevados.
	Comprometimento de uma conta sem privilégios	Comprometimento de um sistema que utiliza contas sem privilégios.
	Comprometimento de aplicações	Comprometimento de uma aplicação através da exploração de vulnerabilidades de <i>software</i> (ex.: <i>SQL injection</i> ).
	DoS ( <i>Denial-of-Service</i> )	Ataque de negação de serviço. Por exemplo: envio de pedidos excessivos a uma aplicação <i>Web</i> que provoque a interrupção ou o abrandamento da prestação do serviço.
	DDoS ( <i>Distributed Denial-of-Service</i> )	Ataque distribuído de negação de serviço.

		Má configuração	Configuração incorrecta do <i>software</i> que causa problemas de disponibilidade do serviço.
Indisponibilidade		Sabotagem	Sabotagem física (ex.: cortes na cablagem do equipamento ou fogo posto)
		Interrupções	Interrupções devidas a causas externas (ex.: catástrofe natural).
		Acesso não autorizado a informações	Acesso não autorizado à informação. Por exemplo: roubo de credenciais de acesso através da interceptação de tráfego ou do acesso a documentos físicos.
Comprometimento de informações		Alteração não autorizada de informações	Alteração não autorizada de informações. Por exemplo: modificação por um atacante utilizando credenciais roubadas de um sistema ou aplicação ou cifragem de dados por <i>ransomware</i> .
		Perda de dados	Perda de informações, por exemplo, devido a uma falha do disco rígido ou roubo físico.
Fraude		Utilização não autorizada de recursos	Utilização de recursos para fins impróprios, incluindo fins lucrativos.
		Direitos de autor	Acesso não autorizado a cópia ou a distribuição ilegal, através da pirataria em <i>software</i> ou violação de direitos em código fonte, protegido por direitos autorais através de meios digitais.
		Falsificação de identidade	Um tipo de ataque em que uma entidade se faz passar por outra para obter ganhos ilegítimos.
		<i>Phishing</i>	Fazer-se passar por outra instituição com o objetivo de convencer o utilizador a revelar credenciais privadas.



**Anexo 3**  
Classificação de Incidentes Quanto aos Níveis de Gravidade

CATEGORIA DE IMPACTO			
	OPERACIONAL	REPUTACIONAL/IMAGEM	FINANCEIRO
<b>Crítico</b>	<ul style="list-style-type: none"> <li>• Interrupção de serviços críticos à médio ou longo prazo (falha =&gt; 200 % do RTO/SLA)</li> <li>• Elevado número de clientes afectados— clientes &gt;=25%.</li> <li>• A resolução/mitigação do incidente implica a activação do Plano de Continuidade de Negócio (PCN).</li> </ul>	<ul style="list-style-type: none"> <li>• Quando o incidente gera exposição negativa nos meios de comunicação internacionais e nas redes sociais.</li> <li>• Reclamações recorrentes, ou seja, repetidas mais de uma vez sobre o mesmo serviço ou produto, indicando persistência do problema.</li> </ul>	<ul style="list-style-type: none"> <li>• Prejuízos financeiros &gt;= 0,5% dos fundos próprios de base Tier I.</li> </ul>
<b>Alto</b>	<ul style="list-style-type: none"> <li>• Indisponibilidade dos activos críticos à médio prazo (100% do RTO/SLA =&lt; falha &lt; 200% do RTO/SLA.</li> <li>• Número de clientes afectados— 10% =&lt; clientes &lt; 25%.</li> <li>• A resolução/mitigação do incidente requer a aplicação de recursos externos.</li> </ul>	<ul style="list-style-type: none"> <li>• Quando o incidente gera ampla exposição negativa nos meios de comunicação nacionais e nas redes sociais, ou provoca reclamações de significativa relevância para a missão institucional.</li> <li>• Reclamações de nível significativo, ou seja, número considerável de reclamações concentradas sobre o mesmo serviço/produto, revelando insatisfação generalizada de clientes.</li> </ul>	<ul style="list-style-type: none"> <li>• Prejuízos financeiros 0,20 % &lt;= dos fundos próprios de base Tier I &lt; 0,50%.</li> </ul>

<b>Médio</b>	<ul style="list-style-type: none"> <li>• Indisponibilidade dos activos críticos à curto prazo (50% do RTO =&lt; falha &lt; 100% do RTO).</li> <li>• Número de clientes afectados– 5% =&lt; clientes &lt; 10%.</li> <li>• A resolução/mitigação do incidente através de recursos internos.</li> </ul>	<ul style="list-style-type: none"> <li>• Quando o incidente provoca exposição negativa limitada nos meios de comunicação nacionais e nas redes sociais, ou gera reclamações de relevância moderada relacionadas à missão institucional.</li> <li>• Reclamações que ocorrem de forma pontual, sem concentração elevada e sem afectar de forma ampla a base de clientes.</li> </ul>	<ul style="list-style-type: none"> <li>• Prejuízos financeiros 0,10 % &lt;= dos fundos próprios de base Tier I &lt; 0,20%.</li> </ul>
<b>Baixo</b>	<ul style="list-style-type: none"> <li>• Indisponibilidade dos activos críticos à curto prazo (falha &lt; 50% do RTO).</li> <li>• Número de clientes afectados - clientes &lt; 5%.</li> <li>• A resolução/mitigação do incidente através de alocação mínima de recursos internos.</li> </ul>	<ul style="list-style-type: none"> <li>• Quando o incidente não possui repercussão nos meios de comunicação nacionais nem nas redes sociais, ou gera reclamações de baixa relevância que não afectam a missão institucional.</li> <li>• Reclamações esporádicas e isoladas, resolvidas rapidamente e sem impacto material na imagem da instituição.</li> </ul>	<ul style="list-style-type: none"> <li>• Prejuízos financeiros &lt; à 0,10% dos fundos próprios de base Tier I.</li> </ul>

**Anexo 4****Lista de Acrónimos**

APT – *Advanced Persistent Threat*  
 DDoS – *Distributed Denial of Service*  
 DoS – *Denial of Service*  
 IDS – *Intrusion Detection System*  
 IPS – *Intrusion Prevention System*  
 RTO – *Recovery Time Objective*  
 SLA – *Service Level Agreement*  
 SPAM – *Sending and Posting Advertisement in Mass*  
 TI – *Tecnologias de Informação*

**Aviso n.º 9/GBM/2025**

de 2 de Dezembro

Havendo necessidade de estabelecer limites para os pagamentos sobre o exterior com recurso a cartões bancários, o Banco de Moçambique, ao abrigo das disposições conjugadas da alínea a) do artigo 9 da Lei n.º 28/2022, de 29 de Dezembro, Lei Cambial e do n.º 4 do artigo 17 da Lei n.º 2/2008, de 27 de Fevereiro, Lei do Sistema Nacional de Pagamentos, determina:

**ARTIGO 1****Objecto**

O presente Aviso estabelece limites de pagamentos sobre o exterior efectuados através de cartões bancários.

**ARTIGO 2****Âmbito**

O presente Aviso aplica-se às instituições de crédito sujeitas à supervisão do Banco de Moçambique e às pessoas singulares e colectivas, titulares de cartões bancários emitidos em Moçambique, independentemente de serem residentes ou não-residentes cambiais.

**ARTIGO 3****Definições**

Para efeitos do presente Aviso, entende-se por:

- a) cartão bancário: instrumento de pagamento, geralmente sob a forma de um cartão de plástico, disponibilizado por uma instituição de crédito ao titular para que este, através do acesso a uma rede de telecomunicações e com base na conta bancária associada ao cartão ou saldo neste carregado, possa realizar operações bancárias. O cartão bancário, de acordo com a sua função, pode ser de crédito, de débito ou pré-pago;
- b) pagamento sobre o exterior: qualquer operação de pagamento realizada sobre o exterior com cartão bancário emitido por uma instituição de crédito autorizada pelo Banco de Moçambique; e
- c) titular: pessoa singular ou colectiva, residente ou não-residente cambial, que celebra com uma instituição de crédito a emissão de cartão bancário e a quem é permitida a sua utilização.

**ARTIGO 4****Limites de pagamentos ao exterior**

1. As pessoas singulares e colectivas só podem efectuar pagamentos sobre o exterior com recurso a cartão bancário até ao limite anual equivalente a 6.000.000,00 MT (seis milhões de meticaís).

2. O limite anual corresponde ao valor agregado em todo o sistema bancário nacional, fixado para cada titular, independentemente do número de contratos celebrados com as instituições de crédito, do número de cartões bancários e dos canais de pagamento pelos quais efectua as transacções, incluindo os levantamentos em numerário.

3. O limite anual não prejudica os limites diários definidos para cada cartão pela instituição de crédito.

4. Atingido o limite fixado no n.º 1, todas as instituições de crédito devem bloquear os cartões bancários, do mesmo titular, para transacções sobre o exterior.

**ARTIGO 5****Fixação de limites pelo Banco de Moçambique**

1. O Banco de Moçambique fixa, caso a caso e mediante pedido, limites diferentes do estabelecido no n.º 1 do artigo anterior.

2. O limite adicional a fixar nos termos do número anterior não deve ultrapassar 6.000.000,00 MT (seis milhões de meticaís).

3. O pedido deve ser fundamentado e submetido pelo titular junto de instituição de crédito à sua escolha, acompanhado da seguinte informação:

- a) Documentos comprovativos do facto gerador da necessidade;
- b) Montante;
- c) Período;
- d) País de destino; e
- e) Outras informações relevantes.

4. A instituição de crédito deve apreciar, emitir o devido parecer e submetê-lo ao Banco de Moçambique no prazo de 5 dias úteis.

5. Recebido o parecer referido no número anterior, o Banco de Moçambique decide no prazo de 15 dias úteis.

**ARTIGO 6****Dever de comunicação**

1. As instituições de crédito devem comunicar aos titulares de cartões bancários, sempre que:

- a) Atingirem a metade do limite anual;
- b) Atingirem o limite anual; e
- c) Bloquearem os cartões bancários.

2. O Banco de Moçambique notifica às instituições de crédito os factos referidos nas alíneas a) e b) do número anterior.

**ARTIGO 7****Aplicação do Regulamento de Cartões Bancários**

Sem prejuízo do disposto no presente Aviso, as instituições de crédito devem observar os deveres previstos no Regulamento de Cartões Bancários aprovado pelo Aviso n.º 1/GBM/2014, de 4 de Junho, alterado e republicado pelo Aviso n.º 10/GBM/2017, de 7 de Junho.