

**Aviso N.º…… /GBM/2024**

**Maputo, … de Outubro de 2024**

|  |  |
| --- | --- |
| **Assunto:** | **Directrizes de reporte de incidentes tecnológicos e cibernéticos** |

Havendo necessidade de estabelecer directrizes de reporte de incidentes tecnológicos e cibernéticos, o Banco de Moçambique, no uso das competências conferidas ao abrigo da 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:

**D****IRECTRIZES DE REPORTE DE INCIDENTES TECNOLÓGICOS E CIBERNÉTICOS**

**CAPÍTULO I**

**DISPOSIÇÕES GERAIS**

Artigo 1

**Objecto**

As presentes Directrizes estabelecem as regras para o reporte de incidentes tecnológicos e cibernéticos.

Artigo 2

**Âmbito de Aplicação**

As presentes Directrizes aplicam-se às instituições de crédito e sociedades financeiras, doravante designadas por “instituições”.

Artigo 3

**Âmbito da informação a reportar**

As instituições financeiras estão sujeitas a reportar os incidentes tecnológicos e cibernéticos, e abrange eventos externos e internos, quer sejam provocados ou acidentais, tendo em conta os níveis de gravidade previstos no Anexo 3.

Artigo 4

**Definições**

Os termos e expressões usados nas presentes Directrizes são definidos no Glossário, em Anexo 1, que é dele parte integrante.

**CAPÍTULO II**

**CLASSIFICAÇÃO DE INCIDENTES**

Artigo 5

**Classificação do incidente quanto à natureza**

As instituições devem considerar a taxonomia apresentada no Anexo 2 nas presentes Directrizes para a classificação da natureza dos incidentes.

Artigo 6

**Classificação do incidente quanto à gravidade**

As instituições devem classificar os incidentes, de acordo com os níveis de gravidade descritos no Anexo 3 das presentes Directrizes.

**CAPÍTULO III**

**REPORTE DE INCIDENTES TECNOLÓGICOS E CIBERNÉTICOS**

Artigo 7

**Modelo de reporte**

1. As instituições devem reportar os incidentes de acordo com os níveis de gravidade descritos no Anexo 3 das presentes Directrizes.
2. Para o cumprimento do disposto no número anterior, 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.
3. Sem prejuízo do estabelecido no número anterior, os incidentes de nível baixo devem estar devidamente documentados e disponíveis para consulta, sempre que se mostrar necessário.

Artigo 8

**Prazo de reporte**

* + - 1. As instituições devem reportar os incidentes de forma incremental nos seguintes prazos máximos:

1. Reporte preliminar: vinte e quatro horas, contadas do momento da sua ocorrência;
2. Reporte intermédio: quarenta e oito horas, contadas do momento da submissão do relatório preliminar; e
3. Reporte final: até trinta dias úteis, após o reporte preliminar.
   * + 1. 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 no futuro.
       2. O plano de acção referido no ponto anterior, é sujeito à avaliação e acompanhamento pelo Banco de Moçambique.

Artigo 9

**Relatório preliminar**

1. O relatório preliminar deve conter informação de caráter geral, descrevendo as características essenciais do incidente e o seu provável impacto, seguindo o modelo aprovado pelo Banco de Moçambique.
2. Sempre que não se encontrem disponíveis dados definitivos, as instituições devem recorrer a estimativas justificáveis para o preenchimento do modelo de reporte.
3. Caso a instituição regresse à normalidade num espaço de tempo inferior ao estabelecido na alínea a) do n.º 1 do artigo anterior, deve submeter todos os relatórios, simultaneamente.

Artigo 10

**Relatório intermédio**

O relatório intermédio deve conter a descrição detalhada do incidente e o seu impacto, devendo ser actualizado sempre que a instituição tiver novas informações relevantes ou alterações significativas.

Artigo 11

**Relatório Final**

O relatório final deve conter a informação que actualiza o relatório intermédio e adiciona 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 12

**Reporte agregado**

As instituições devem remeter mensalmente, até ao dia quinze, a relação dos incidentes ocorridos no mês anterior, devendo para o efeito juntar:

1. Carta de remessa, devidamente assinada por um membro do Conselho de Administração e pelo executivo sénior responsável pela gestão dos incidentes;
2. Informação agregada dos incidentes ocorridos dentro do período considerado, conforme Modelo aprovado por Circular.

Artigo 13

**Informações adicionais**

O Banco de Moçambique pode solicitar às instituições informações adicionais, bem como realizar averiguações que considere necessárias sobre o estado dos incidentes cibernéticos reportados.

Artigo 14

**Preservação de informação e dever de colaboração**

As instituições devem preservar os dados e evidências relacionadas com a ocorrência dos incidentes reportados, bem como colaborar com as autoridades reguladoras e de segurança, no âmbito da investigação dos referidos incidentes.

**CAPÍTULO V**

**DISPOSIÇÕES FINAIS**

Artigo 15

**Regime Sancionatório**

O incumprimento do previsto nas presentes Directrizes constitui contravenção punível nos termos da Lei das Instituições de Crédito e Sociedades Financeiras.

Artigo 16

**Entrada em vigor**

As presentes Directrizes entram em vigor noventa dias a contar da data da sua publicação.

Artigo 17

**Esclarecimento de dúvidas**

As dúvidas na interpretação e aplicação das presentes Directrizes devem ser submetidas ao Departamento de Supervisão Prudencial do Banco de Moçambique.

**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 dos dados e na reputação da instituição.

**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, 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.

**M**

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

**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 transacções 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**

***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 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 *patches*, 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. |
| Incidente Tecnológico (cont.) | Falhas de equipamento | Configuração incorrecta | Parametrizações inadequadas de equipamentos. |
| Obsolescência | Equipamento obsoleto e fora do período de suporte. |
| 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. |
| *Firmware* não actualizado | Falta de actualização do *software* embutido em *hardware.* |
| Outros | Qualquer incidente que não se enquadra em nenhuma das categorias anteriores. |
| Falhas/Interrupção da infraestrutura de redes de comunicações | Erros/falhas de equipamentos de Rede | Falha em *switches*, roteadores, *firewalls* 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 internet ou provedor de serviço | Interrupção do serviço de internet e problemas em conexões de Backup. |
|  | Falhas/Interrupção da infraestrutura de redes de comunicações (cont.) | 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 switches e configurações de DNS e DHCP. |
| Falhas em equipamentos de comunicação *wireless* | Problemas em Pontos de Acesso Wi-Fi 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. |
| Incidente Cibernético | Conteúdo abusivo  Conteúdo abusivo (cont) | *Spam* | Correio electrónico em massa não solicitado. O destinatário do conteúdo não deu uma autorização válida para receber uma mensagem em massa. |
| Crimes de ódio, crimes contra a liberdade ou a honra | Conteúdo difamatório ou discriminatório. Por exemplo: *cyberbullying*, racismo, ameaças a uma pessoa ou dirigidas a grupos, entre outro. |
| Pornografia infantil, conteúdos sexuais ou violentos | Material que apresente visualmente conteúdos relacionados com pornografia infantil, apologia da violência, entre outros. |
| Código malicioso | *Worm* | *Software* que é intencionalmente incluído ou inserido num sistema com finalidade prejudicial. Normalmente, é necessária uma interacção do utilizador para activar o código. |
| *Trojan* |
| *Spyware* |
| *Dialler* |
| *Rootkit* |
| Recolha de informações | *Scanning* | Ataques que enviam pedidos a um sistema para descobrir pontos fracos. Isto inclui também algum tipo de processos de teste para recolher informações sobre *hosts*, serviços e contas. |
| *Sniffing* | Observação e registo do tráfego da rede (escutas telefónicas). |
| Engenharia social | Técnicas utilizadas para obter informações confidenciais através de ações que enganam ou exploram a confiança das pessoas. |
| Tentativa de intrusão | Exploração de vulnerabilidades conhecidas | Uma tentativa de comprometer um sistema ou de perturbar qualquer serviço através da exploração de vulnerabilidades. |
| 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. |
| Ataque desconhecido | Tentativa de utilizar uma exploração desconhecida. |
| Intrusão | 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 software. Por exemplo, SQL *injection*. |
| Indisponibilidade | DoS (*Denial-of-Service*) | Ataque de negação de serviço. Por exemplo: envio de pedidos excessivos a uma aplicação Web que provoque a interrupção ou o abrandamento da prestação do serviço. |
| DDoS (*Distributed* *Denial-of-Service*) | Ataque distribuído de negação de serviço. |
| Má configuração | Configuração incorrecta do *software* que causa problemas de disponibilidade do serviço. |
| Sabotagem | Sabotagem física. Por exemplo: cortes na cablagem do equipamento ou fogo posto |
| Interrupções | Interrupções devidas a causas externas. Por exemplo: catástrofe natural. |
| Comprometimento de informações | Acesso não autorizado a informações | Acesso não autorizado à informação. Por exemplo: roubo de credenciais de acesso através da intercepção de tráfego ou do acesso a documentos físicos. |
| 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 *ransomware*. |
|  | 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 *software* 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. |
| *Phishing* | Fazer-se passar por outra instituição com o objetivo de convencer o utilizador a revelar credenciais privadas. |
| Vulnerabilidade | Criptografia fraca | Serviços acessíveis ao público que podem ter uma criptografia fraca. |
| Amplificador DDoS | Serviços acessíveis ao público que podem ser utilizados para a reflexão ou amplificação de ataques DDoS. |
| Divulgação de informações | Acesso público a serviços em que podem ser divulgadas informações potencialmente sensíveis. |
|  | Serviços com potencial de acesso não desejado | Funcionalidades em sistemas, redes ou dispositivos que podem ser exploradas para permitir acesso não autorizado. |
| Sistema vulnerável | Falhas de segurança ou fraquezas, resultantes de erros de programação, configurações inadequadas, falta de actualizações de segurança, ou *design* inadequado, que podem ser exploradas para comprometer sistemas organizacionais. . |
| Outros | APT (*Advanced Persistent Threat*) | Forma de ataque cibernético caracterizada por sua sofisticação, persistência e foco específico em alvos seleccionados, como organizações ou entidades governamentais. Esta ameaça emprega normalmente técnicas de engenharia social para atingir os seus objectivos, juntamente com a utilização de procedimentos de ataque conhecidos ou genuínos. |
| Outros | Qualquer incidente que não se enquadra em nenhuma das categorias anteriores. |

**ANEXO 3**

**CLASSIFICAÇÃO DE INCIDENTES QUANTO AOS NÍVEIS DE GRAVIDADE**

|  |  |
| --- | --- |
| **Nível** | **Descrição** |
| **Crítico** | * Danos extensos e prolongados aos objectivos de protecção (disponibilidade, integridade, confidencialidade) dos activos críticos presentes ou previstos. * Disponibilidade: os activos críticos não estão disponíveis à médio ou longo prazo (falha => 200 % do RTO[[1]](#footnote-1)). * Disponibilidade de sistemas: cujo impacto resulta na indisponibilidade total de aplicações principais e periféricas ao serviço dos clientes. * Abrangência: repercutido a nível da rede nacional. * A resolução/mitigação do incidente implica a activação do Plano de Continuidade de Negócio (PCN). |
| **Alto** | * Disponibilidade: os activos críticos não estão disponíveis a médio prazo (100% do RTO =< falha < 200% do RTO). * Abrangência: afectou a rede regional/sede. * Disponibilidade de sistemas: provocam indisponibilidade parcial de algumas aplicações principais e periféricas perturbando a qualidade de entrega de serviços/aplicações ao cliente. * Confidencialidade/integridade: informações sensíveis e/ou críticas para o negócio comprometidas em grande medida. * A resolução/mitigação do incidente requer a aplicação de recursos externos. |
| **Médio** | * Disponibilidade: os activos críticos não estão disponíveis a curto prazo (50% do RTO =< falha < 100% do RTO). * Abrangência: repercutido a nível local (balcões). * Disponibilidade de sistemas: causa interrupção ou perturbação de sistemas para efeitos de manutenção dos sistemas. * Confidencialidade/integridade: informações sensíveis substancialmente afectadas. * Implicações financeiras perceptíveis ou danos na reputação da instituição. * O incidente pode ser resolvido com os recursos internos disponíveis. |
| **Baixo** | * Sem prejuízo aos objectivos de protecção (disponibilidade, integridade, confidencialidade) dos activos críticos. * Disponibilidade: activos críticos sofrem pequenas oscilações (falha < 50% do RTO) * Abrangência: afectou apenas algumas funcionalidades e não causou interrupção. * Disponibilidade de sistemas: provoca pequenas oscilações dos sistemas sem impacto na disponibilidade de serviços/aplicações para os clientes. * Não há redução da capacidade da instituição para cumprir efectivamente as suas obrigações.   Não há danos, ou há danos mínimos, ao património da instituição, sejam eles financeiros, de informação, de imagem ou de qualquer outra natureza. |

**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 Objectives* |
| SPAM | *Sending and Posting Advertisement in Mass* |
| TI | Tecnologias de Informação |

1. RTO: *Recovery Time Objective* [↑](#footnote-ref-1)