BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRENSA 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 1/GBM/2024

de 15 de Março

Havendo necessidade de estabelecer normas sobre fundos próprios e limites prudenciais para as empresas prestadoras de serviços de pagamentos, o Banco de Moçambique, no uso das competências que lhe são conferidas pelo n.º 1 do artigo 80, n.º 1 do artigo 85 e n.º 2 do artigo 90, todos da Lei n.º 20/2020, de 31 de Dezembro, Lei das Instituições de Crédito e Sociedades Financeiras, determina:

CAPÍTULO I

Disposições Gerais

ARTIGO 1

Objecto

O presente Aviso estabelece as normas sobre fundos próprios e limites prudenciais das empresas prestadoras de serviços de pagamentos.

ARTIGO 2

Âmbito de aplicação

O presente Aviso aplica-se às empresas prestadoras de serviços de pagamentos.

CAPÍTULO II

Normas Prudenciais

SECÇÃO I

Fundos Próprios

ARTIGO 3

Composição dos fundos próprios

Os fundos próprios das empresas prestadoras de serviços de pagamentos são constituídos por elementos positivos e negativos, nos termos definidos pelos artigos 4 e 5 do presente Aviso.

ARTIGO 4

Elementos positivos dos fundos próprios

São considerados elementos positivos dos fundos próprios os seguintes:

a) capital realizado, incluindo a parte representada por acções preferenciais não remíveis;
b) prémios de emissão de acções e de outros títulos;
c) reservas legais, estatutárias e outras formadas por resultados não distribuídos;
d) resultados positivos transitados de exercícios anteriores;
e) resultados positivos do último exercício, nas condições referidas no artigo 11;
f) resultados positivos provisórios do exercício em curso, nas condições referidas no artigo 11;
g) parcela das reservas e dos resultados correspondentes a activos por impostos diferidos;
h) elementos caracterizados no artigo 12, cujas condições sejam aprovadas pelo Banco de Moçambique;
i) elementos caracterizados no artigo 13;
j) reservas provenientes da reavaliação dos activos fixos tangíveis, efectuada nos termos do Diploma Legal que a autorize;
k) empréstimos subordinados, nas condições referidas no artigo 14; e
l) parte liberada de acções preferenciais remíveis.

ARTIGO 5

Elementos negativos dos fundos próprios

São considerados elementos negativos dos fundos próprios os seguintes:

a) acções próprias, pelo valor de inscrição no balanço;
b) outros elementos próprios enquadráveis no artigo anterior, pelo valor de inscrição no balanço;
c) activos intangíveis;
d) resultados negativos transitados de exercícios anteriores;
e) resultados negativos do último exercício;

2. Como parte do quadro referido no número anterior, as empresas prestadoras de serviços de pagamento devem estabelecer:

a) procedimentos de identificação, avaliação e acompanhamento do risco operacional intrínseco aos seus produtos, serviços e sistemas significativos;
b) o nível de tolerância ao risco;
c) procedimentos para o controlo e mitigação do risco;
d) procedimentos eficazes de gestão de incidentes, inclusive para a detecção e classificação de incidentes operacionais e de segurança de carácter severo; e
e) planos de recuperação de desastres e de continuidade de negócios.

3. As empresas prestadoras de serviços de pagamento devem fornecer ao Banco de Moçambique, anualmente e sempre que for solicitada, uma avaliação exaustiva e actualizada dos riscos operacionais e de segurança, bem assim da adequação das medidas de mitigação dos riscos e dos mecanismos de controlo aplicados em resposta a esses riscos.

ARTIGO 26

Comunicação de incidentes

No caso de ocorrência de um incidente operacional ou de segurança de carácter severo, as empresas prestadoras de serviços de pagamento devem:

a) notificar imediatamente o Banco de Moçambique; e
b) se o incidente tiver ou for susceptível de ter repercussões nos interesses financeiros dos seus utilizadores de serviços de pagamento, informá-los, imediatamente, do incidente e de todas as medidas que aqueles podem tomar para atenuar os seus efeitos adversos.

CAPÍTULO IV

Disposições Finais e Complementares

ARTIGO 27

Remessa de Informação

As empresas prestadoras de serviços de pagamento devem remeter ao Banco de Moçambique:

a) o mapa de fundos próprios, com referência ao último dia de cada mês e dentro dos 15 dias seguintes;
b) o mapa dos rácios e limites prudenciais, trimestralmente; e,
c) até ao dia 15 de cada mês:
i. o saldo de contas fiduciárias e respectivo rácio de concentração de depósitos;
ii. o saldo dos juros de contas fiduciárias; e
iii. o total dos saldos pendentes de moeda electrónica por si detidos e respectivo rácio sobre os saldos de conta fiduciária.

ARTIGO 28

Regime sancionatório

A violação das disposições do presente Aviso constitui contravenção prevista e punível nos termos da Lei n.º 20/2020, de 31 de Dezembro.

ARTIGO 29

Esclarecimento de dúvidas

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

ARTIGO 30

Prazo de adequação

As instituições devem conformar os seus actos e procedimentos às disposições constantes do presente Aviso, no prazo de 180 dias, a contar da data da sua entrada em vigor.

ARTIGO 31

Entrada em vigor

O presente Aviso entra em vigor 90 dias após a data da sua publicação.

Banco de Moçambique, em Maputo, aos 25 de Janeiro 2024. — Governador, *Rogério Lucas Zandamela.*

Aviso n.º 2/GBM/2024

de 15 de Março

Havendo necessidade de estabelecer directrizes para a mitigação do risco cibernético, com o objectivo de, por um lado, promover a governação e gestão deste risco no sector financeiro, e por outro, prever os requisitos para as instituições aperfeiçoarem a sua postura no que diz respeito à resiliência cibernética, 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:

1. São aprovadas as Directrizes de Gestão do Risco e Resiliência Cibernética, que fazem parte integrante do presente Aviso.

2. O presente Aviso entra em vigor 180 dias após a data da sua publicação.

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

Banco de Moçambique, em Maputo, aos 31 de Janeiro de 2024. — Governador, *Rogério Lucas Zandamela*.

Directrizes de Gestão do Risco e Resiliência Cibernética

CAPÍTULO I

Disposições Gerais

ARTIGO 1

Objecto

As presentes Directrizes estabelecem o quadro geral de governação, gestão do risco e resiliência cibernética.

ARTIGO 2

Âmbito

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

ARTIGO 3

Proporcionalidade

Na aplicação das Directrizes, as instituições devem adoptar uma abordagem baseada no risco e projectar os esforços de mitigação, de modo que as medidas a implementar sejam proporcionais ao seu nível de exposição ao risco cibernético.

ARTIGO 4

Definições

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

ARTIGO 5

Auto-avaliação do risco cibernético

1. As instituições devem realizar a auto-avaliação dos seus processos de gestão de risco e resiliência cibernética, tendo em conta as componentes previstas no artigo 7 das presentes Directrizes e remeter os respectivos resultados ao Banco de Moçambique, bem como o Plano de Remediação.

2. Os documentos referidos no número anterior devem ser elaborados com referência a 31 de Dezembro do ano anterior e remetidos ao Banco de Moçambique até ao dia 31 de Março do ano seguinte à que reporta.

ARTIGO 6

Reporte de Incidentes

As instituições devem reportar os incidentes cibernéticos no prazo máximo de 24 horas, contadas do momento da sua ocorrência, pela via e no modelo determinados pelo Banco de Moçambique.

CAPÍTULO II

Gestão do Risco e Resiliência Cibernética

SECÇÃO I

Componentes

ARTIGO 7

Componentes de gestão do risco cibernético

1. A Gestão do Risco Cibernético contempla 9 domínios, designadamente:

a) governação;
b) identificação;
c) protecção;
d) detecção;
e) resposta e recuperação;
f) consciência situacional;
g) teste;
h) terceirização (*outsourcing*); e
i) aprendizagem e evolução.

2. No âmbito das componentes de gestão de Risco Cibernético, entende-se por:

a) Governação: mecanismos implementados pelas instituições com o objectivo de viabilizar o estabelecimento, implementação e revisão da abordagem de gestão do risco cibernético;
b) Identificação: processo pelo qual as instituições devem identificar, classificar, registar e actualizar todas as suas funções críticas e respectivas interconexões, incluindo os activos de informação, funções do pessoal-chave e processos que suportam essas funções. Esta acção visa permitir que a instituição priorize os processos de protecção, detecção, resposta e recuperação para cada uma destas funções;
c) Protecção: conjunto de controlos, sistemas e processos de segurança que as instituições implementam para proteger a confidencialidade, integridade e disponibilidade da informação;
d) Detecção: conjunto de medidas que permite às instituições reconhecer sinais de potenciais incidentes cibernéticos ou detectar intrusões ocorridas;
e) Resposta e recuperação: mecanismos que permitem às instituições retomar as funções críticas rapidamente, em segurança e com dados precisos, por forma a mitigar os riscos de falha potencialmente sistémicos;
f) Consciência situacional: práticas que permitem às instituições compreenderem o ambiente de ameaças cibernéticas em que operam, as implicações para seu negócio e a adequação de suas medidas de mitigação do risco cibernético. As práticas permitem a construção de um forte nível de consciencialização e compromisso para assegurar a resiliência cibernética global;
g) Teste: um conjunto de medidas que as instituições põem em prática para identificar lacunas nos objectivos de resiliência e fornecer pontos de entrada significativos para o processo de gestão do risco cibernético;
h) Terceirização (*Outsourcing*): medidas através das quais se espera que as instituições incorporem a resiliência cibernética ao desenvolver e actualizar a sua estrutura de *outsourcing* e que considerem o risco cibernético associado e o risco decorrente da interligação do ecossistema financeiro; e
i) Aprendizagem e evolução: práticas através das quais as instituições asseguram que os seus programas de segurança cibernética atingem uma contínua resiliência cibernética dentro de um cenário de ameaças dinâmico, de modo a tornarem-se eficazes no acompanhamento da rápida evolução das ameaças.

SECÇÃO II

Governação

ARTIGO 8

Estratégia e *framework*

1. As instituições devem estabelecer uma estratégia e um *framework* de segurança cibernética adaptados à sua natureza, dimensão, perfil de risco cibernético e cultura.

2. A estratégia e o *framework* de segurança cibernética devem especificar como identificar, gerir e reduzir efectivamente os riscos cibernéticos de uma forma integrada e abrangente.

3. A estratégia e o *framework* de segurança cibernética devem ser estabelecidos, mantidos e adaptados aos riscos cibernéticos específicos e devidamente orientados por normas nacionais do sector e boas práticas internacionais.

ARTIGO 9

Gestão do risco cibernético

1. A gestão do risco cibernético deve ser estabelecida como parte integrante do programa de gestão do risco organizacional, no qual as instituições avaliam o risco cibernético inerente às pessoas, processos, tecnologia, actividades, produtos e serviços identificados.

2. As instituições devem identificar os riscos e avaliar a existência e eficácia dos controlos de protecção contra o risco identificado, com vista a apurar o risco residual.

3. O risco cibernético deve ser devidamente identificado, classificado e mapeado através de um cenário que considere tanto o agente interno como externo, de modo a que sejam implementados controlos como medidas de tratamento e mitigação deste risco.

4. As instituições devem considerar o facto do risco cibernético poder variar consoante o modelo de negócio da instituição, seus parceiros, prestadores de serviços e fornecedores e não necessariamente de acordo com o seu grau de relevância.

ARTIGO 10

Papéis e responsabilidades

As instituições devem definir as responsabilidades das diferentes funções envolvidas na gestão do risco, nomeadamente:

a) definir, de forma clara, as responsabilidades de todas as funções de gestão e fiscalização, incluindo as linhas de defesa, bem como os comités necessários para a fiscalização do risco cibernético;

b) assegurar que a gestão do risco cibernético seja incorporada nas suas estruturas, processos e procedimentos de governação e gestão de risco, incluindo disposições relativas às linhas de reporte directo ao órgão da administração; e

c) garantir que seja estabelecida uma função de segurança cibernética com recursos adequados, autoridade apropriada e que tenha acesso ao órgão da administração, sempre que aplicável.

ARTIGO 11

Estratégia de segurança cibernética

1. As instituições devem estabelecer e manter uma estratégia de segurança cibernética aprovada pelo órgão da administração e alinhada com as suas estratégias globais.

2. A estratégia de segurança cibernética deve compreender:

a) a importância da resiliência cibernética para a instituição;

b) os requisitos de alto nível das partes interessadas;

c) A visão e missão da instituição relativamente à resiliência cibernética;

d) os objectivos da resiliência cibernética;

e) o apetite ao risco cibernético;

f) as metas de resiliência cibernética e o respectivo plano de implementação;

g) o âmbito de alto nível da tecnologia e dos activos utilizados para gerir a resiliência cibernética;

h) o modo como iniciativas de resiliência cibernética são entregues, geridas e financiadas;

i) a integração da resiliência cibernética em pessoas, processos, tecnologia e iniciativas institucionais novas ou já existentes;

j) gestão de dados; e

k) consciencialização sobre segurança cibernética.

3. Para incorporar as possíveis alterações ao nível do panorama de ameaças cibernéticas, alocar recursos, identificar e corrigir lacunas e incorporar as lições aprendidas, as instituições devem rever a estratégia de segurança cibernética, pelo menos, anualmente.

ARTIGO 12

Políticas e procedimentos de segurança cibernética

1. Com periodicidade mínima anual, as instituições devem definir e quantificar a tolerância do negócio com relação ao risco cibernético e assegurar que esta esteja consistente com a estratégia e o apetite de risco organizacional.

2. As instituições devem estabelecer métricas para recolher informações que permitam a elaboração de relatórios, tanto ao nível técnico como executivo, em todos os aspectos do seu programa de implementação da gestão do risco cibernético.

ARTIGO 13

Responsabilidades do órgão de administração

1. O órgão de administração é responsável, em última instância, por:

a) assegurar que a instituição cumpra os requisitos estabelecidos nas presentes Directrizes; e

b) fiscalizar a gestão do risco cibernético, podendo delegar a função primariamente a um comité existente ou criado para o efeito.

2. O órgão de administração deve ainda:

a) assegurar, em coordenação com órgãos da gestão de topo, o estabelecimento de uma estratégia e *framework* de segurança cibernética sólidos e robustos, e a respectiva implementação;

b) garantir que a gestão de topo colabore com outras partes interessadas, conforme relevante e apropriado, a fim de assegurar a resiliência cibernética do sistema;

c) assegurar que as funções e responsabilidades referentes à segurança estejam claramente definidas no contrato ou no Acordo de Nível de Serviço (*Service Level Agreement* - SLA) com prestadores de serviços terceirizados;

d) assegurar a realização da auto-avaliação do risco cibernético; e

e) assegurar a eficácia e eficiência da auditoria interna no âmbito da avaliação dos processos sujeitos a risco cibernético ou do acompanhamento de trabalhos e recomendações de auditorias e certificações externas.

ARTIGO 14

Responsabilidades da gestão de topo

1. A gestão de topo deve garantir que um executivo sénior seja responsável pela implementação da estratégia e estrutura de gestão de risco e resiliência cibernética ao nível institucional.

2. A gestão de topo deve apresentar, pelo menos, anualmente, um relatório escrito ao órgão de administração sobre o estado global do risco e resiliência cibernética.

3. Para efeitos do número 1 do presente artigo, a gestão de topo deve garantir que o executivo sénior:

a) tenha actuação independente;

b) possua acesso directo ao órgão de administração; e

c) tenha competências, conhecimento e experiência adequados em matéria de especialidade.

ARTIGO 15

***Framework* de segurança cibernética**

O *framework* de segurança cibernética deve:

a) incorporar, no mínimo, as seguintes áreas:

i. identificação, incluindo a classificação e risco de activos;

ii. protecção, incluindo os controlos lógicos e físicos;

iii. segurança de recursos humanos;

iv. gestão de alterações e *patches*;

v. gestão de terceiros;

vi. detecção;

vii. mecanismos de gestão de incidentes de segurança cibernética;

viii. resposta e recuperação;

ix. testes;

x. consciência situacional;

b) definir como as instituições estabelecem a sua tolerância ao risco e objectivos cibernéticos e como identificam, mitigam e gerem o seu risco cibernético;

c) incorporar as directrizes do presente Aviso relacionadas com a governação, capacitação e gestão de riscos de terceiros;

d) ser elaborado, tendo em conta os componentes referidos no artigo 7 do presente Aviso, e estar alinhado às normas (*standards*) e boas práticas internacionais orientadas para o sector financeiro;

e) ser consistente com o *framework* organizacional de gestão de risco;

f) ser revisto, pelo menos, anualmente, de modo a verificar a adequação e eficácia dos controlos, através de programas de conformidade independentes e auditorias realizadas por indivíduos qualificados; e

g) determinar os controlos necessários para manter o risco dentro do apetite estabelecido.

SECÇÃO III

Identificação

ARTIGO 16

Deveres das instituições

1. As instituições devem:

a) identificar os processos de negócio, as funções críticas e os activos de informação que suportam o negócio e a entrega de serviços, incluindo os geridos por provedores de serviços terceirizados;

b) classificar os processos de negócio e activos de informação em termos de criticidade e sensibilidade, que, por sua vez, devem orientar a priorização da sua protecção, detecção e resposta;

c) realizar, anualmente, avaliações de risco sobre as funções críticas e activos de informação de suporte, por forma a assegurar que não estejam comprometidos e que estejam protegidos contra dependências externas, de modo a determinar prioridades entre estes;

d) manter um inventário actualizado, pelo menos, anualmente, de todas as funções críticas, funções-chave, processos, activos de informação, fornecedores de serviços terceirizados e interligações;

e) integrar esforços na identificação de outros processos relevantes, como aquisição e gestão de alterações, com o objectivo de facilitar uma revisão regular do seu inventário;

f) criar e manter um inventário actualizado, revisto, pelo menos anualmente, de todas as contas individuais e de sistema, de modo a incluir as contas com acesso remoto ou direitos de acesso privilegiado, a fim de assegurar que o acesso à informação sensível e aos sistemas de suporte seja mantido, apenas quando necessário;

g) identificar e documentar todos os processos que estão dependentes da relação com provedores de serviços terceirizados e identificar as suas interligações, devendo a informação ser actualizada, sempre que aplicável;

h) conduzir avaliações do risco cibernético antes da introdução ou actualização de tecnologias, produtos, serviços ou processos, de modo a identificar atempadamente ameaças ou vulnerabilidades associadas;

i) criar e manter a topologia de rede e conectividade interna e externa que inclui recursos que suportam as funções críticas; e

j) salvaguardar que a governação e fiscalização da função de segurança cibernética seja independente das operações no seu reporte, por forma a assegurar uma adequada segregação de funções e evitar quaisquer potenciais conflitos de interesses.

2. A topologia de rede referida na alínea *i*) do número anterior deve ser actualizada, sempre que se mostre necessário.

ARTIGO 17

Gestão de Activos

1. As instituições domésticas de importância sistémica devem assegurar a implementação de soluções automatizadas de gestão de activos que possibilitem a rastreabilidade e correlação entre os serviços, produtos prestados e os activos que os suportam, tanto *hardware* como *software*, de modo a possibilitar a identificação do ponto de falha, em caso de disrupção ou indisponibilidade destes serviços.

2. O Banco de Moçambique avalia caso a caso e sempre que as circunstâncias assim determinarem, a necessidade de implementação pelas demais instituições de soluções automatizadas de gestão de activos, nos termos previstos na presente disposição.

SECÇÃO IV

Protecção

ARTIGO 18

Capacidades de resiliência cibernética

As instituições devem criar capacidade de resiliência cibernética e implementar práticas de segurança cibernética, que sejam adequadas e eficazes para prevenir, limitar ou conter o impacto de um potencial evento cibernético.

ARTIGO 19

Objectivos de segurança cibernética

1. As instituições devem implementar um conjunto abrangente e apropriado de controlos de segurança que permitam alcançar os objectivos de segurança cibernética, de modo a responder os seus requisitos de negócio, com base na identificação das suas funções críticas, papéis-chave, processos, activos de informação, fornecedores de serviços de terceiros e interligações, de acordo com a avaliação de risco na fase de identificação.

2. Os objectivos de segurança cibernética devem assegurar:

a) a continuidade e disponibilidade dos sistemas de informação e a protecção da integridade da informação armazenada nos seus sistemas, tanto em utilização como em trânsito;

b) a protecção, integridade, confidencialidade e disponibilidade dos dados em estado de armazenamento, utilização e trânsito; e

c) a conformidade com as leis, regulamentos e outras normas aplicáveis.

3. As instituições devem actualizar, pelo menos anualmente, os seus controlos de segurança cibernética, por forma a assegurar que as abordagens adoptadas se mantêm proporcionais às suas funções críticas, ao cenário de ameaça cibernética e à importância sistémica.

ARTIGO 20

Monitorização de sistemas

As instituições devem monitorizar os seus sistemas ao longo do seu ciclo de vida, para identificar fraquezas e garantir que:

a) todas as actualizações disponíveis sejam instaladas de forma atempada e segura, sendo mantidas, adequadamente, com o devido suporte;

b) são implementadas e testadas camadas adicionais de segurança cibernética, onde são identificadas vulnerabilidades nos sistemas; e

c) são descartados e substituídos todos os sistemas desactualizados, com suporte limitado ou sem suporte ou com vulnerabilidades que não podem ser corrigidas ou mitigadas, adequadamente, por meio da segregação de outros sistemas.

ARTIGO 21

Gestão de acessos

1. As instituições devem garantir a gestão adequada de acessos, assegurando:

a) a limitação de acesso dos activos de informação e instalações associadas à utilizadores, processos e dispositivos autorizados, de acordo com o princípio da segregação de deveres e privilégios mínimos, concedendo acesso mínimo apenas àqueles que tenham uma necessidade legítima;

b) a implementação de controlos que limitam e monitoram, de forma rigorosa, o pessoal com maior nível de privilégio ou direitos de acesso;

c) acriação de processos com vista a monitorizar o acesso ao sistema e à informação e accionar alertas em caso de tentativas de acesso não autorizado;

d) que o acesso aos activos de informação e instalações associadas é gerido de forma proporcional à avaliação do risco de acesso não autorizado;

e) a implementação de políticas e procedimentos de segurança, bem como o estabelecimento de mecanismos de gestão de identidade e de controlo de acesso, para proporcionar uma administração eficaz e consistente dos utilizadores, responsabilização e autenticação, de modo a:

i. garantir que o acesso remoto aos activos de informação apenas é permitido a partir de dispositivos protegidos, de acordo com as normas de segurança das instituições;

ii. assegurar que é implementada uma autenticação forte para os utilizadores que efectuam o acesso remoto, por forma a salvaguardar o acesso não autorizado ao ambiente informático;

iii. sujeitar os prestadores de serviços e terceiros com acesso aos activos de informação à mesma monitorização e restrições de acesso concedida aos seus colaboradores;

iv. estabelecer um processo que permita gerir e controlar a utilização de sistemas informáticos e contas de serviços em caso de actividades suspeitas ou não autorizadas;

v. implementar processos visando assegurar a monitorização dos colaboradores face às mudanças de funções ou cessação de contratos de trabalho, de modo a garantir que, em caso de mudança de responsabilidades do colaborador, todos os direitos de acesso relacionados com a posição anterior e não necessários para as novas funções são revogados atempadamente;

vi. implementar rastreios (*screening*) e verificações de antecedentes baseados no risco para todos os novos colaboradores e terceiros, antes da sua contratação; e

vii. assegurar que os colaboradores em posições sensíveis, designadamente, aqueles que mudam para funções que requerem acesso privilegiado a sistemas críticos ou que se tornam pessoal de alto risco, sejam pré-seleccionados.

2. Atendendo às suas atribuições e ao significativo nível de risco cibernético a que estão expostos, devem ser fornecidas formações e treinamentos personalizados ao pessoal com maior privilégio ou funções de administrador de sistemas ou redes, referido na alínea *b*) do número 1 do presente artigo.

ARTIGO 22

Gestão de alterações

1. As instituições devem possuir políticas, procedimentos e controlos para a gestão de alterações que:

a) incluam critérios de prioridade e classificação destas, designadamente, alteração normal *versus* alteração de emergência;

b) estipulem que, previamente à qualquer alteração, as instituições assegurem que o respectivo pedido é:

i. revisto, a fim de satisfazer as necessidades de negócio;

ii. categorizado e avaliado por forma a identificar potenciais riscos e assegurar que não tem um impacto negativo na confidencialidade, integridade, disponibilidade e nos sistemas e dados da instituição;

iii. aprovado pelo nível de gestão adequado;

iv. definido um plano de retorno em caso de falha e/ou processo mal sucedido. e

c) certifiquem que a equipa de segurança cibernética é envolvida ao longo do ciclo de vida do processo de gestão de alterações.

2. As instituições devem testar, validar e documentar as alterações aos sistemas de informação antes da sua implementação em produção, podendo incluir testes de integração e testes de aceitação pelo utilizador, entre outros.

3. As alterações aos sistemas de informação devem incluir, mas não se limitar, a modificação de componentes de *hardware*, *software* ou *firmware* e definições de configuração do sistema e de segurança cibernética.

4. As instituições devem assegurar a existência de processos que permitem a programação da implementação das alterações e comunicação aos afectados antes da implementação efectiva, incluindo a sua consulta, sempre que aplicável.

ARTIGO 23

Gestão de *patches*

1. As instituições devem ter uma política e processos abrangentes de gestão de *patches* que incluam:

a) a identificação de *patches* apropriados para sistemas específicos;

b) a análise do impacto da sua instalação e no caso de se verificarem incumprimentos das recomendações dos fornecedores;

c) regras que assegurem que os *patches* sejam instalados correctamente, previamente testados e monitorados após a instalação; e

d) a documentação de todos os procedimentos associados, como configurações específicas exigidas.

2. As instituições devem considerar o uso de configuração de base (*standard*) de recursos de Tecnologias de Informação, de modo a facilitar o processo de gestão de *patches*.

3. As instituições devem assegurar que a instalação de novos *patches* tenha a aprovação prévia do nível de gestão adequado.

ARTIGO 24

Situações de emergência

1. As instituições devem possuir processos para identificar, avaliar e aprovar alterações provenientes de situações de emergência.

2. As instituições devem conduzir revisões pós-implementação para validar os procedimentos de emergência adoptados e determinar o impacto da alteração de emergência.

ARTIGO 25

Salvaguardas

As instituições devem possuir políticas e procedimentos que salvaguardam a proibição de alterações e instalação de *patches* que não tenham sido pré-aprovadas.

ARTIGO 26

Controlos de segurança de dados

1. As instituições devem implementar controlos de segurança de dados que permitam:

a) prevenir a perda de dados e adoptar medidas para detectar e evitar o acesso não autorizado, modificação, cópia ou transmissão dos dados sensíveis em trânsito, armazenados ou em utilização;

b) proteger os dispositivos terminais, através da implementação de medidas apropriadas para prevenir e detectar o furto de dados e modificações não autorizadas;

c) assegurar que os sistemas informáticos geridos por prestadores de serviços e terceiros possuam o mesmo nível de protecção e são sujeitos às mesmas normas de segurança cibernética implementadas ao nível da instituição;

d) certificar que os dados sensíveis armazenados em sistemas e dispositivos terminais são codificados e protegidos por fortes mecanismos de controlo de acesso;

e) salvaguardar que apenas os sistemas informáticos autorizados, dispositivos terminais e meios de armazenamento de dados são utilizados para comunicar, transferir ou armazenar dados sensíveis;

f) prevenir e detectar a utilização de serviços de *Internet* não autorizados que permitam aos utilizadores comunicar ou armazenar dados sensíveis;

g) assegurar que a utilização de dados de produção sensíveis em ambientes não produtivos é restringida;

h) salvaguardar que os dados sensíveis são permanentemente apagados dos meios de armazenamento, sistemas informáticos e dispositivos terminais, antes destes serem descontinuados ou redistribuídos;

i) salvaguardar que, no caso de rescisão de contrato com determinado provedor, é prevista a devolução ou transferência segura de dados ou, caso esta devolução seja impossível, são previstos mecanismos que permitam a destruição segura dos suportes de armazenamento que contenham informação da instituição.

2. As instituições devem, no âmbito do controlo de segurança de dados, estabelecer acordos de não-divulgação de informação ou de confidencialidade com os utilizadores.

3. Em situações excepcionais, caso os dados de produção referidos na alínea *g*) do número anterior sejam utilizados em ambientes não produtivos, devem existir processos adequados para o pedido de dados e a aprovação deve ser obtida junto da gestão superior.

ARTIGO 27

Controlos de segurança de aplicações e sistemas

As instituições devem adoptar controlos de segurança de aplicações e de sistemas, com o objectivo de:

a) implementar uma abordagem de segurança por projecto referente à incorporação de controlos de segurança em cada fase do desenvolvimento de aplicações, com objectivo de:

i. minimizar as vulnerabilidades do sistema;

ii. reduzir as possibilidades de ataque;

b) determinar o nível aceitável de segurança necessário para satisfazer as necessidades de negócio e avaliar as potenciais ameaças e riscos relacionados com o sistema;

c) assegurar que os requisitos de segurança relativos ao controlo de acesso ao sistema, autenticação, autorização de transacção, integridade dos dados dos *logs*, monitorização dos eventos de segurança e tratamento de excepções são, claramente, especificados nas fases iniciais de desenvolvimento ou aquisição do sistema; e

d) assegurar que as aplicações críticas do negócio (sistemas *core*) são revistas e testadas, de modo a garantir que não exista impacto adverso nas operações ou na segurança, quando são efectuadas alterações a tais aplicações.

ARTIGO 28

Controlos de segurança de rede

1. As instituições devem incorporar controlos de segurança de rede, através de:

a) instalação de dispositivos de segurança para proteger a rede, entre elas e *Internet* e as ligações com prestadores de serviços;

b) implantação de sistemas de detecção ou prevenção de intrusão na rede para detectar e bloquear o tráfego malicioso;

c) revisão da arquitectura de rede, incluindo a concepção da sua segurança e das respectivas interligações numa base periódica, de modo a identificar potenciais vulnerabilidades;

d) implementação de controlos de acesso à rede para detectar e impossibilitar a ligação de dispositivos não autorizados à sua rede;

e) segregação física e/ou lógica dos seus dispositivos terminais que permitem acesso à *Internet* ou implementação de controlos equivalentes, proibindo e bloqueando o acesso dos terminais privilegiados, como, terminais de pagamento SWIFT; e

f) encriptação das ligações remotas, de modo a prevenir fugas de dados, através de ataques como os relacionados com a varredura de rede (tais como *network sniffing* e *eavesdropping*).

2. As regras de controlo de acesso à rede em dispositivos de rede referidos na alínea *d*) do número anterior devem ser revistas pelo menos anualmente, de modo a assegurar que se mantêm actualizadas.

ARTIGO 29

Criptografia

1. Na implementação da criptografia, as instituições devem:

a) estabelecer políticas, normas e procedimentos de gestão de chaves criptográficas abrangendo a geração, distribuição, instalação, renovação, revogação, recuperação e expiração de chaves;

b) adoptar algoritmos criptográficos conformes com as normas internacionais estabelecidas;

c) garantir que as chaves criptográficas são geradas com segurança e protegidas contra divulgação não autorizada em sistemas reforçados e são resistentes a adulterações;

d) utilizar um método seguro de destruição de chaves, por forma a assegurar que não são recuperáveis quando expiradas ou revogadas;

e) determinar a duração de vida apropriada de cada chave criptográfica, com base em factores, como:

i. a sensibilidade dos dados;

ii. a criticidade do sistema a ser protegido;

iii. as ameaças e riscos a que os dados ou sistema podem estar expostos;

f) manter as cópias de segurança das chaves criptográficas para fins de recuperação e adopção de um elevado nível de protecção, de modo a evitar que as mesmas sejam corrompidas ou apagadas involuntariamente; e

g) garantir que todos os algoritmos criptográficos utilizados são sujeitos à testes ou verificações rigorosas, de modo a cumprir com os objectivos e requisitos de segurança identificados.

2. Qualquer chave criptográfica, gerada nos termos da alínea *c*) do número anterior, ou dados confidenciais usados para gerar ou derivar as chaves devem ser protegidos ou destruídos com segurança, após a geração da mesma.

3. A chave criptográfica referida na alínea *e*) do número 1 do presente artigo deve ser substituída com segurança, antes da mesma expirar.

SECÇÃO V

Detecção

ARTIGO 30

Incidentes cibernéticos

1. As instituições devem manter uma capacidade efectiva de resiliência cibernética, por forma a reconhecer sinais de um potencial incidente cibernético ou detectar a ocorrência de um comprometimento real.

2. As instituições devem definir, considerar e documentar o perfil de base das actividades do sistema por forma a detectar prováveis desvios, designadamente, actividades e eventos anómalos.

3. As instituições devem desenvolver os recursos apropriados, incluindo humanos, processos e tecnologia, para monitorizar e detectar actividades e eventos anómalos, definindo critérios, parâmetros e gatilhos (*triggers*) apropriados para habilitar alertas.

4. As instituições devem estabelecer processos de monitorização sistemática para detectar, de forma atempada, incidentes cibernéticos e avaliar, de forma contínua, a eficácia dos controlos identificados, inclusive por meio da monitorização, testes, auditorias e exercícios à rede.

5. Para efeitos do disposto no número anterior, a detecção atempada deve assegurar que as instituições tenham um tempo apropriado para implementar medidas adequadas contra potenciais intrusões e permitir a contenção proactiva destas.

ARTIGO 31

Monitorização das actividades dos sistemas informáticos e análise contínua

1. As instituições devem monitorizar as actividades dos sistemas informáticos, de modo a detectar ataques ou iniciativas de ataques aos seus sistemas e serviços de negócio e responder de forma eficiente e atempada, nomeadamente:

a) estabelecer um sistema de monitorização e análise contínua de eventos cibernéticos, nomeadamente, através de um Centro de Operações de Segurança (*Security Operations Center - SOC*) ou equivalente e a detecção e rápida resposta a incidentes cibernéticos;

b) definir processos, papéis e responsabilidades para as operações de segurança;

c) estabelecer um processo de recolha, revisão e retenção de *logs* de sistemas de segurança, de modo a facilitar as operações de monitorização de segurança, e proteger os respectivos registos contra o acesso não autorizado; e

d) garantir que os recursos de detecção e monitorização, bem como as linhas de base de desempenho do sistema, critérios de activação e alertas são revistos, testados e actualizados, tendo em atenção o alinhamento com os outros testes dos sistemas, por forma a assegurar a precisão no rastreio de riscos cibernéticos.

2. As instituições devem implementar ferramentas de monitorização contínua de vulnerabilidades, por forma a identificar, classificar e tratar em tempo útil, as vulnerabilidades classificadas como de nível de risco alto e/ou crítico, de acordo com os prazos estabelecidos em procedimentos internos da instituição.

3. As instituições devem assegurar que as suas capacidades de detecção e monitorização permitem a recolha de informação suficiente para apoiar a investigação de eventos e incidentes cibernéticos

ARTIGO 32

Configuração de eventos ou alertas

1. As instituições devem configurar eventos ou alertas dos sistemas informáticos, por forma a fornecer indicadores antecipados de aspectos que possam afectar o seu desempenho e segurança.

2. Os eventos ou alertas devem ser activamente monitorizados para que as instituições tomem medidas imediatas para resolver atempadamente os problemas detectados.

3. As instituições devem efectuar a correlação de múltiplos eventos registados nos *logs* dos sistemas informáticos, como forma de identificar padrões de actividades suspeitas ou anómalas.

ARTIGO 33

Processo de escalonamento

As instituições devem estabelecer um processo de escalonamento atempado para as partes interessadas relativamente às actividades suspeitas ou anómalas do sistema ou comportamento do utilizador.

ARTIGO 34

Camadas de controlo de detecção

1. As instituições devem incorporar múltiplas camadas nos seus controlos de detecção, incluindo pessoas, processos e tecnologia.

2. Os controlos referidos no número anterior devem ter a capacidade de detectar ataques cibernéticos e isolar o ponto de comprometimento.

SECÇÃO VI

Resposta e recuperação

ARTIGO 35

Mecanismos de resposta

1. As instituições devem implementar mecanismos para responder e recuperar, rapidamente, de ataques cibernéticos, bem como mitigar os potenciais riscos sistémicos.

2. Após a detecção de um ataque cibernético ou de uma tentativa, a instituição deve efectuar uma investigação exaustiva para determinar a sua natureza e extensão, bem como os danos ocorridos e tomar medidas imediatas para conter a situação, por forma a prevenir danos adicionais e iniciar os esforços de recuperação a fim de restaurar as operações, com base no seu plano de resposta.

ARTIGO 36

Políticas e processos de gestão de incidentes

As instituições devem estabelecer políticas e processos eficazes de gestão de incidentes que permitam:

a) aprimorar a resiliência;
b) assegurar a continuidade de funções e/ou serviços críticos;
c) melhorar a confiança dos clientes e de partes interessadas; e
d) potencialmente, reduzir qualquer impacto.

ARTIGO 37

Estratégia de *backup*

1. As instituições devem estabelecer uma estratégia de *backup* e desenvolver um plano de realização de *backups*, de modo que os dados possam ser recuperados, em caso de interrupção ou nos casos em que estes sejam corrompidos ou apagados.

2. A instituição deve ainda garantir que todos os dados sensíveis, armazenados nos dispositivos de *backup*, são protegidos, entre outros mecanismos, através da encriptação.

3. Os dispositivos de *backup* devem ser armazenados em um local externo que não esteja sujeito aos mesmos riscos que a fonte de dados.

ARTIGO 38

Estratégia de comunicação

1. As instituições devem implementar uma estratégia de comunicação clara com os clientes afectados por ataques cibernéticos, incluindo detalhes sobre as alternativas disponíveis para mitigar o impacto.

2. A estratégia de comunicação deve incluir:

a) canais de comunicação directos, fiáveis e seguros com as partes interessadas, para a troca de informação; e
b) mecanismos padronizados de comunicação com os seus clientes, em caso de ataques cibernéticos dedicados a este grupo, nomeadamente os ataques de engenharia social tais como *phishing, smishing, vishing*, especificando, de forma objectiva, a informação que deve ou não ser comunicada aos clientes, através dos seus vários canais de comunicação, como a exclusão de *links* clicáveis nas comunicações da instituição.

ARTIGO 39

Objectivos de ponto e de tempo de recuperação

As instituições devem definir os seus Objectivos de Ponto de Recuperação (*Recovery Point Objectives* - RPO) e de Tempo de Recuperação (*Recovery Time Objectives* - RTO) proporcionais às suas necessidades do negócio e ao seu papel sistémico no ecossistema económico-financeiro, de modo a permitir a tomada das melhores decisões sobre os seus objectivos de recuperação, na eventualidade de um incidente cibernético.

ARTIGO 40

Plano de resposta e gestão de incidentes cibernéticos

1. As instituições devem desenvolver um plano de resposta e gestão de incidentes cibernéticos para isolar e neutralizar prontamente uma ameaça cibernética e reestabelecer, com segurança, os serviços afectados.

2. O plano deve descrever os procedimentos de comunicação, coordenação e resposta para lidar com cenários de ameaças cibernéticas.

3. As instituições devem garantir que o plano de resposta e gestão de incidente cibernético alcance os objectivos de recuperação, prioridades de restauração e determine as capacidades necessárias para a disponibilidade contínua do sistema, com base em diferentes cenários cibernéticos.

4. O plano deve definir funções e responsabilidades e estabelecer opções para redireccionar ou substituir funções ou serviços críticos que possam estar afectados por um ataque cibernético bem-sucedido por um período significativo.

5. As instituições devem ter procedimentos necessários que visam assegurar a rápida recuperação, em caso das alterações ou correcções falharem.

6. Qualquer alteração no ambiente de produção deve estar consubstanciada por um plano de recuperação associado.

ARTIGO 41

Testagem dos planos

1. As instituições devem testar, regularmente, os seus planos de resposta aos incidentes cibernéticos, abrangendo diversos cenários.

2. A periodicidade dos testes referidos no número anterior deve estar alinhada aos testes realizados no Plano de Continuidade de Negócios da instituição.

ARTIGO 42

Processos de resposta e recuperação

As instituições devem dispor de processos de resposta e recuperação de incidentes cibernéticos, incluindo:

a) ambientes de simulação de incidentes cibernéticos integrados com a gestão de crises, continuidade do negócio, planeamento da recuperação de desastres e operações de recuperação;
b) procedimentos para colectar e rever a informação de seus incidentes de segurança cibernética e resultados de testes, por forma a melhorar, continuamente, os seus planos de contingência, resposta, retomada e recuperação;

c) processos para realizar análises, a posterior, das causas dos incidentes de segurança cibernética, devendo as constatações das análises ser integradas nos planos de resposta, retoma e recuperação de incidentes cibernéticos; e
d) procedimentos para a retoma da actividade.

SECÇÃO VII

Consciencialização situacional

ARTIGO 43

Entendimento sobre as ameaças

As instituições devem compreender todo o conjunto de ameaças e as suas implicações no ambiente em que operam, bem como a adequação das suas medidas de mitigação de riscos cibernéticos.

ARTIGO 44

Cultura de consciencialização

1. As instituições devem promover uma cultura institucional que reconheça que o pessoal, a todos os níveis, tem responsabilidades importantes para assegurar a resiliência cibernética, através de uma comunicação interna clara e efectiva, que inclua a partilha de informação relevante sobre a estratégia e *framework* cibernético a todos os colaboradores.
2. As instituições devem promover uma cultura de consciencialização em matérias de risco cibernético para os seus clientes.

ARTIGO 45

Formação

1. As instituições devem assegurar:
a) a existência de um programa de formação contínua e testes de consciencialização sobre o risco e resiliência cibernética para todo o pessoal;
b) a cobertura, pelo programa de formação, sem prejuízo de outros, da realização de testes de engenharia social, incluindo falsas campanhas de *e-mails* de *phishing*;
c) o equilíbrio adequado de competências, conhecimentos e experiência para compreender e avaliar os riscos cibernéticos que enfrentam.

2. As instituições devem elaborar programas de consciencialização e educação dos clientes em matérias de literacia cibernética, de modo a dotá-los de técnicas de detecção de comunicações fraudulentas.

ARTIGO 46

Recolha de informação

1. As instituições devem estabelecer um processo de recolha de informação relativa aos riscos cibernéticos de fontes internas e externas pela sua relevância e potencial impacto no negócio e no ambiente de tecnologias de informação, com o objectivo de manter uma boa consciência da situação de risco cibernético.
2. Para efeitos do disposto do número anterior, consideram-se fontes internas e externas as seguintes:
a) *logs* de aplicações, sistemas e redes;
b) dispositivos de segurança, tais como *firewalls* e Sistemas de Detecção de Intrusões (*Intrusion Detection Systems* - IDS); e
c) fornecedores fiáveis de informações sobre ameaças;
d) informação pública disponível.

ARTIGO 47

Análise da informação

As instituições devem analisar toda a informação recolhida para gerar um entendimento relevante sobre ameaças cibernéticas e para utilizá-la, continuamente, para avaliar e gerir as ameaças e vulnerabilidades de segurança, com o objectivo de implementar controlos adequados de segurança cibernética nos seus sistemas e, a um nível geral, reforçar o seu quadro de resiliência cibernética e as suas capacidades numa base contínua.

ARTIGO 48

Partilha de informação

As instituições devem participar activamente nos grupos e recursos de partilha de informação existentes, incluindo grupos inter-profissionais, inter-governamentais e transfronteiriços para recolher, distribuir e avaliar informação sobre práticas cibernéticas, ameaças cibernéticas e indicadores de alerta prévio relacionados com ameaças cibernéticas.

ARTIGO 49

Metas e objectivos de partilha de informação

1. As instituições devem definir metas e objectivos de partilha de informação, de acordo com os seus objectivos de negócio e seu quadro de resiliência cibernética.
2. No mínimo, os objectivos devem incluir a recolha e troca de informação de forma atempada que facilite a detecção, resposta, retoma e recuperação dos seus sistemas e de outros integrantes do sector durante e após um ataque cibernético.

SECÇÃO VIII

Testes

ARTIGO 50

Testes da resiliência cibernética

As instituições devem testar todos os elementos da sua capacidade de resiliência cibernética e controlos de segurança para determinar a eficácia global e verificar se:
a) estão implementados correctamente;
b) funcionam como pretendido; e
c) produzem os resultados desejados.

ARTIGO 51

Natureza e frequência dos testes

1. A natureza e a frequência dos testes devem ser proporcionais aos seguintes elementos:
a) ritmo a que as vulnerabilidades e ameaças mudam;
b) criticidade e sensibilidade do sistema informático ou da informação;
c) consequências de um incidente de segurança;
d) riscos associados à exposição a ambientes em que as instituições são incapazes de aplicar as suas políticas de segurança; e
e) materialidade e frequência das alterações aos activos de informação.

2. As instituições devem avaliar a natureza e a frequência dos testes dos controlos sobre os activos de informação que são geridos por prestadores de serviços terceirizados.

ARTIGO 52

Tipos de testes

1. Dependendo do perfil de risco cibernético, dimensão, estrutura de governação, ambiente operativo, complexidade, sofisticação de produtos e serviços e interligação com outras entidades, as instituições devem realizar os seguintes testes:

a) avaliações de vulnerabilidades;
b) baseados em cenários;
c) de intrusão; e
d) de *Red Teaming e Threat Led Penetration Test* (TLPT).

2. Após a realização dos testes referidos nas alíneas *c*) e *d*) do número anterior, as instituições devem adoptar medidas correctivas para mitigar as deficiências, vulnerabilidades e riscos identificados.

ARTIGO 53

Comunicação ao órgão de administração

O órgão de administração deve ser comunicado sobre quaisquer resultados de testes que identifiquem deficiências de controlo de segurança que não possam ser corrigidas em tempo útil.

ARTIGO 54

Garantia do controlo de segurança cibernética

As instituições devem assegurar que o controlo de segurança cibernética é efectuado por pessoal devidamente qualificado.

ARTIGO 55

Avaliações de vulnerabilidades

1. As instituições devem estabelecer um processo de realização de avaliações de vulnerabilidades nos seus sistemas informáticos, para identificar vulnerabilidades de segurança e assegurar que os riscos decorrentes das mesmas são tratados atempadamente.

2. A frequência das avaliações de vulnerabilidades deve ser proporcional à criticidade dos sistemas informáticos e aos riscos de segurança a que estes estão expostos.

3. Para efeitos do disposto no número anterior, os processos de avaliações devem ser realizados, pelo menos, trimestralmente para as instituições domésticas de importância sistémica e semestralmente para as demais.

4. As instituições devem garantir que as ferramentas utilizadas para as avaliações de vulnerabilidades sejam fidedignas e com perfis de *scanning* actualizados mensalmente.

ARTIGO 56

Testes baseados em cenários

1. As instituições devem realizar exercícios de simulação baseados em cenários, com periodicidade anual, para validar as suas capacidades de resposta e recuperação, bem como os seus planos de comunicação, contra as ameaças cibernéticas prevalecentes.

2. Na concepção do exercício de simulação, as instituições devem utilizar informação de ameaça que seja relevante para o seu ambiente de negócio, a fim de identificar:

a) os agentes mais susceptíveis de representar ameaça; e
b) as tácticas, técnicas e procedimentos mais susceptíveis de serem utilizados em tais ataques.

ARTIGO 57

Testes de Intrusão

1. As instituições devem realizar testes de intrusão para obter avaliação aprofundada das suas defesas de segurança cibernética e para validar a adequação dos controlos de segurança dos sistemas informáticos e dos activos de informação directamente acessíveis a partir da *Internet*, pelo menos anualmente ou sempre que tais sistemas e activos sofram alterações ou actualizações materiais.

2. Na realização dos testes de intrusão, as instituições devem:

a) assegurar a combinação de testes de *black box, grey box and white box* para sistemas informáticos e activos de informação; e
b) documentar os resultados e definir planos de acção para a mitigação das vulnerabilidades identificadas.

3. A frequência dos testes de intrusão é determinada com base em factores como a criticidade e a exposição a riscos cibernéticos.

ARTIGO 58

Testes de *Red Teaming* e TLPT

1. Após a implementação das medidas que mitigam devidamente as deficiências detectadas, através das avaliações de vulnerabilidade, testes baseados em cenários e testes de intrusão, as instituições domésticas de importância sistémica devem:

a) realizar, pelo menos anualmente, exercícios independentes de *Red Teaming*, nomeadamente:

i. execução de ataques controlados de engenharia social;
ii. plantação de dispositivos. e

b) desafiar as funções críticas sobre possíveis vulnerabilidades e a eficácia de controlos de mitigação, incluindo o seu pessoal, processos e tecnologia.

2. A *Red Team* deve testar a forma como a equipa de segurança da instituição responde às várias ameaças.

3. Para a materialização do disposto no número anterior, a *Red Team* deve ser uma equipa independente da equipa de segurança cibernética, devendo ser constituída por pessoal interno e/ou peritos externos.

4. Compete ao Banco de Moçambique determinar, em instrumento específico, os critérios para a realização do TLPT pelas instituições domésticas de importância sistémica.

5. O teste referido no número anterior deve ser conduzido por entidades com certificações acreditadas e independentes das instituições.

6. Para efeitos do disposto no número 1 do artigo 52, o Banco de Moçambique avalia, caso a caso, e sempre que as circunstâncias assim o determinem, a sujeição das demais instituições à realização dos testes previstos no presente artigo.

ARTIGO 59

Controlos de gestão de remediação

1. Após a realização dos testes ou exercícios de segurança cibernética, as instituições devem estabelecer controlos de gestão de remediação com o objectivo de:

a) criar um processo de remediação abrangente para acompanhar e resolver problemas identificados a partir dos testes ou exercícios de segurança cibernética, das avaliações de terceiros, das auto-avaliações e das constatações de avaliações internas e externas;
b) assegurar que todos os problemas identificados a partir da realização de testes ou exercícios de segurança cibernética, bem como as deficiências de *software*

detectadas a partir da revisão do código fonte e dos testes de segurança da aplicação, são rastreados e os principais problemas e defeitos de *software* são remediados antes da colocação em produção; e

c) manter um registo das actualizações e vulnerabilidades relatadas sobre *software* de terceiros e de código aberto por si utilizados, a fim de facilitar a remediação das vulnerabilidades de forma atempada.

2. O processo referido na alínea *a*) do número anterior deve, no mínimo, incluir:

a) avaliações da gravidade e a classificação dos problemas;

b) prazos para remediar os problemas de gravidade diferente;

c) avaliações de risco, sempre que necessário; e

d) estratégias de mitigação para gerir desvios do *framework* de segurança cibernética.

SECÇÃO IX

Terceirização

ARTIGO 60

Avaliação

As instituições devem avaliar a criticidade e sensibilidade das actividades, dados ou processos a terceirizar e realizar uma avaliação de risco, antes de celebrar qualquer contrato de terceirização.

ARTIGO 61

Dever de diligência

1. As instituições devem realizar a devida diligência e documentar os resultados associados antes de assinar qualquer contrato, com o objectivo de avaliar a capacidade de terceiros para cumprir a especificação de resiliência cibernética.

2. Ao realizar a devida diligência, as instituições devem ter acesso aos relatórios de auditoria ou resultados de certificações de avaliações independentes de fornecedores que suportam funções críticas, como forma de avaliar o perfil do prestador de serviços de terceiros quanto a segurança cibernética.

ARTIGO 62

Identificação do risco cibernético

As instituições devem identificar e documentar, de forma clara, o risco cibernético associado à utilização de fornecedores de serviços de terceiros e actualizar, pelo menos, anualmente.

ARTIGO 63

Contratação de terceiros

As instituições devem assegurar que os contratos que celebram com terceiros contemplam requisitos de segurança cibernética proporcionais ao seu apetite ao risco, que incluam, no mínimo:

a) papéis e responsabilidades de cada parte envolvida relativamente ao acesso aos dados;

b) resposta e comunicação de incidentes;

c) gestão da continuidade do negócio;

d) cessação do contrato;

e) portabilidade dos dados; e

f) acesso aos relatórios de auditoria e relatórios de certificações de avaliações independentes.

ARTIGO 64

Sub-contratações

1. As instituições devem ser devidamente informadas sobre quaisquer sub-contratações feitas por prestadores de serviços com os quais tenham um acordo de terceirização.

2. A instituição pode permitir a sub-contratação, por seus prestadores de serviços, apenas quando os sub-contratados possam cumprir, integralmente, as obrigações existentes entre ambos.

ARTIGO 65

Portabilidade e interoperabilidade de dados

As instituições devem ter em conta a portabilidade e interoperabilidade dos seus dados e aplicações e incluir disposições nos seus contratos de terceirização por forma a evitar o bloqueio (*lock-in*) pelo fornecedor.

ARTIGO 66

Deveres

Sem prejuízo de outros deveres indicados na presente Subsecção, as instituições devem:

a) conceber e verificar os controlos de segurança para detectar e prevenir possíveis intrusões decorrentes de ligações de terceiros;

b) assegurar que o acesso aos seus dados confidenciais pelos colaboradores de prestadores de serviços é activamente rastreado e controlado, com base no princípio de privilégios mínimos;

c) integrar, no seu plano de resposta, terceiros que prestam serviços para as suas funções críticas; e

d) assegurar que para as funções críticas, previstas na alínea *c*) do n.º 1 do artigo 16 do presente Aviso, os seus Planos de Continuidade de Negócio contemplam mecanismos de transição para prestadores de serviços alternativos ou de realização interna das funções.

SECÇÃO X

Aprendizagem e Evolução

ARTIGO 67

Identificação e avaliação de ameaças

1. As instituições devem ter processos que permitam identificar e avaliar ameaças e vulnerabilidades de segurança e tomar medidas para as gerir de uma forma adaptativa e dinâmica.

2. As instituições devem ainda identificar e classificar as lições estratégicas, tácticas e operacionais aprendidas e identificar, sistematicamente, as principais partes interessadas a quem estas se aplicam, incorporá-las na melhoria do *framework* e das capacidades de resiliência cibernética e transmiti-las à cada parte interessada relevante, numa base contínua.

ARTIGO 68

Desenvolvimentos tecnológicos e formação

1. As instituições devem acompanhar activamente os desenvolvimentos tecnológicos e manter-se a par dos novos processos de gestão de riscos cibernéticos que podem mitigar eficazmente as formas de ataques cibernéticos existentes e recentemente desenvolvidas.

2. As instituições devem incorporar as lições aprendidas na formação do pessoal, nos programas e materiais de sensibilização, de forma contínua e dinâmica.

ARTIGO 69

Definição de indicadores

1. As instituições devem definir um conjunto de indicadores e desenvolver informação de gestão para medir e monitorar a efectiva implementação da estratégia e *framework* de resiliência cibernética, numa base anual, e a sua evolução ao longo do tempo.

2. Nos termos do disposto no número anterior, consideram-se indicadores, mas não se limitam, os seguintes:

a) percentagem do pessoal que recebeu formação em segurança cibernética;

b) Percentagem de incidentes reportados dentro do prazo exigido por categoria;

c) Percentagem de vulnerabilidades mitigadas dentro de um período de tempo definido após a descoberta; e

d) Relatórios anuais de monitorização do progresso dos indicadores.

Anexo

Glossário

a) **Abordagem baseada no risco:** abordagem através da qual as instituições identificam, avaliam e compreendem os riscos aos quais estão expostas e tomam as medidas comensuradas com os riscos identificados;

b) **Activo de informação:** qualquer porção de dados, dispositivos ou outros componentes do ambiente que suporta actividades relacionadas com a informação, incluindo dados, *hardware* e *software*. Os activos de informação não estão limitados apenas àqueles detidos pela instituição, estando incluídos, também, os que são alugados ou contratados e aqueles que são utilizados pelos provedores de serviços para fornecerem os seus serviços;

c) **Ameaça cibernética:** uma circunstância ou evento com o potencial de, intencionalmente ou não, explorar uma ou mais vulnerabilidades nos sistemas de uma instituição, resultando na perda da confidencialidade, integridade ou disponibilidade;

d) **Ataque cibernético:** o uso de uma vulnerabilidade para obter vantagem de uma ou mais fraquezas com o intuito de infligir um efeito adverso no ambiente de tecnologias de informação e comunicação;

e) **Centro de Operações de Segurança (*Security Operations Center* - SOC):** uma função ou serviço responsável pela monitorização, detecção e contenção de incidentes;

f) **Consciencialização situacional:** a capacidade de identificar, processar e compreender os elementos críticos de informação através do processo de inteligência das ameaças cibernéticas que fornece um nível de entendimento relevante para agir sobre a mitigação do impacto de um potencial evento malicioso;

g) **Disponibilidade:** a propriedade de ser acessível e utilizável como esperado quando necessário;

h) **Dispositivos Terminais:** qualquer dispositivo que pode se conectar à rede da instituição;

i) ***Eavesdropping:*** prática de escuta ou espionagem não autorizada, onde ocorre uma interceptação não autorizada de comunicações electrónicas. Considerada uma ameaça à confidencialidade e à privacidade de dados;

j) **Ecossistema:** um conjunto de todos os elementos interligados e interdependentes que interagem num determinado ambiente, podendo incluir instituições, reguladores, provedores de serviços terceiros, fornecedores de bens, clientes, entre outros;

k) **Estratégia de segurança cibernética:** conjunto de planos, políticas, procedimentos e medidas adoptados por uma instituição para proteger seus sistemas de informação e activos contra ameaças cibernéticas;

l) **Evento cibernético:** ocorrência observável num sistema de informação ou rede;

m) **Funções críticas:** qualquer actividade, função, processo ou serviço cuja perda, mesmo que por um curto período, afecte materialmente a operação contínua de uma instituição, dos seus participantes, do mercado que serve ou todo o sistema financeiro;

n) ***Framework* de segurança cibernética:** consiste nas políticas, procedimentos e controlos que as instituições estabeleceram para identificar, proteger, detectar, responder e recuperar de fontes plausíveis de risco cibernético que a mesma enfrenta;

o) **Gestão do risco cibernético:** processo usado pelas instituições para estabelecer um *framework* corporativo de gestão da probabilidade de ataques cibernéticos e desenvolver estratégias para coordenar a mitigação, resposta e aprendizado de ataques cibernéticos;

p) **Gestão de topo:** entes responsáveis por desenhar e implementar estratégias de negócio e gestão dos riscos a que uma instituição está exposta, conforme orientações emanadas do órgão de administração;

q) **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;

r) **Incidente de segurança:** qualquer violação física ou digital que ameaça a confidencialidade, integridade ou disponibilidade dos sistemas de informação ou dados confidenciais de uma instituição. Os incidentes podem variar desde ataques cibernéticos conduzidos por *hackers* ou utilizadores não autorizados, até violações não intencionais da política de segurança por utilizadores legitimamente autorizados;

s) **Indicador:** uma ocorrência ou sinal que revele que um incidente ocorreu ou está em curso;

t) **Integridade:** refere-se à garantia de que os dados ou informações não foram alterados de forma não autorizada, intencional ou acidental. Os sistemas e dados são considerados íntegros quando permanecem completos, precisos e confiáveis ao longo do tempo.

u) ***Intrusion Detection System*:** sistema que monitora redes de comunicações com objectivo de encontrar eventos que possam violar as regras de segurança daquelas e subsequentemente, gera alertas aos administradores de sistemas;

v) ***Logs* (trilhas de auditoria):** que também pode ser chamada de trilhas de auditoria, são registos detalhados e cronológicos de actividades ou eventos significativos num sistema, rede ou aplicativo, cuja principal finalidade é de permitir a monitoria e análise

das acções realizadas por utilizadores, aplicativos, sistemas e processos.

w) ***Network sniffing*:** consiste, no contexto de ataque cibernético, num acto malicioso não autorizado de capturar e analisar pacotes de dados numa rede, com o objectivo de obter informações confidenciais ou sensíveis. É um método utilizado para obter informações sobre o tráfego, identificar problemas de rede, realizar análises de segurança;

x) **Parte Interessada:** pessoa ou organização que pode afectar, ser afectada ou considerar-se como sendo afectada por uma decisão ou actividade, podendo ser um indivíduo ou um grupo que tem um interesse em qualquer decisão ou actividade de uma organização;

y) ***Patches***: actualizações ou correcções de *software* fornecidas pelo provedor da aplicação, por forma a melhorar o seu uso ou performance;

z) **Perfil de risco cibernético:** o risco cibernético assumido e mensurado num determinado momento;

aa) ***Phishing*:** tipo de ataque cibernético que envolve o uso de técnicas de engenharia social para enganar e manipular as vítimas, com o objectivo de obter informações confidenciais, como senhas, informações bancárias, números de cartões de crédito e outras informações pessoais. Neste tipo de ataque, os criminosos fazem-se passar por entidades confiáveis, como bancos, empresas de serviços, redes sociais, provedores de *e-mail* ou até mesmo colegas de trabalho;

bb) **Plano de Remediação:** conjunto de medidas a serem apresentadas e implementadas pela instituição, face as situações de inconformidade identificadas durante as avaliações internas (auto-avaliações) ou acções de inspecção. O Plano de Remediação deve apresentar acções específicas para solucionar cada inconformidade e respectivo prazo;

cc) **Plano de Retorno (Plano de *Rollback* ou Plano de Resolução):** um plano que inclui, obrigatoriamente, toda alteração, independentemente do tipo, dimensão e complexidade. Este plano deve ser activado, no caso em que ocorrem falhas durante a implementação de determinada alteração comprometendo o objectivo da missão, onde as configurações devem ser alteradas, de modo a reflectir configurações iniciais. Estas actividades devem ser devidamente planeadas e testadas;

dd) **Política:** conjunto formal de princípios e padrões que traduzem o comportamento desejado e orientam a actuação de uma instituição, conforme expectativas expressas do órgão de administração;

ee) **Programa de gestão do risco:** descrição formal do sistema de governação e processos de gestão de riscos estabelecidos na instituição;

ff) **Protecção:** desenvolvimento e implementação das salvaguardas, controlos e medidas apropriadas visando garantir a provisão de serviços de infra-estruturas críticas;

gg) **Recuperação:** A restauração de quaisquer funcionalidades ou serviços afectados devido a eventos cibernéticos;

hh) ***Red team*:** um grupo independente que desafia a resiliência cibernética de uma instituição para testar as suas defesas e melhorar a sua efectividade e analisar a resiliência cibernética de uma instituição numa perspectiva de adversário;

ii) ***Recovery Point Objectives* (RPO):** quantidade máxima aceitável de volume/dados que podem ser perdidos a partir do instante em que ocorre um desastre, falha ou um evento de perda de dados, medido em termos de quantidade de tempo;

jj) ***Recovery Time Objectives* (RTO):** tempo aceitável em que um sistema pode ficar indisponível após um desastre. Esta métrica é uma previsão máxima estipulada para restaurar um sistema, serviço, aplicação ou rede após a ocorrência de um incidente ou falha;

kk) **Resposta:** capacidade de a instituição desenvolver e implementar as actividades apropriadas para estar capaz de tomar as devidas acções quando detectados eventos cibernéticos;

ll) **Resiliência cibernética**: capacidade das instituições para antecipar, aguentar, conter e rapidamente recuperar de um ataque cibernético;

mm) **Restauração:** o reinício das funções após a ocorrência dum incidente cibernético. A instituição deve restaurar os serviços críticos logo que se mostre seguro e praticável de o fazer sem causar o risco desnecessário para o sector ou mais danos a estabilidade financeira. O plano de acção deve considerar a utilização de instalações secundárias (*sites* secundários) e ser desenhado para garantir que os sistemas críticos de tecnologias de informação e comunicação podem restaurar as operações dentro do RTO estabelecido pela instituição;

nn) **Risco cibernético:** a combinação da probabilidade da ocorrência de um evento dentro do contexto dos activos de informação, computadores e recursos de comunicações de uma instituição e as consequências desse evento para a mesma;

oo) ***Smishing:*** combinação das palavras "SMS" e "*phishing*". É um tipo de ataque cibernético, assim como no *phishing* tradicional, que utiliza técnicas de engenharia social para enganar e manipular as vítimas, mas, nesse caso, é realizado através de mensagens de texto (SMS) enviadas para os dispositivos móveis das potenciais vítimas. Neste tipo de ataque, os golpistas enviam mensagens de texto falsas ou fraudulentas para as vítimas, fazendo-se passar por entidades confiáveis, como bancos, empresas de serviços, órgãos governamentais ou outras organizações respeitáveis;

pp) ***Threat Led Penetration Test* (TLPT):** tentativa controlada de comprometer a resiliência cibernética de uma instituição através da simulação de tácticas, técnicas e procedimentos de actores de ameaças da vida real, baseando-se na inteligência da ameaça direccionada e concentrando-se em pessoas, processos e tecnologia, com um mínimo de previdência e impacto nas operações;

qq) **Tolerância ao risco:** disposição da instituição ou das partes interessadas para assumir o risco após o seu o tratamento, por forma a poder alcançar os seus objectivos;

rr) **Tolerância ao risco cibernético:** disposição de uma instituição em aceitar e gerir os riscos relacionados à segurança da informação e aos ataques cibernéticos de forma estratégica e consciente. É uma abordagem que busca equilibrar a protecção adequada dos activos

e informações com as prioridades, metas e recursos disponíveis da instituição;

ss) ***Vishing:*** combinação das palavras "*voice*" (voz) e "*phishing*", portanto variante do ataque cibernético *phishing*, que utiliza técnicas de engenharia social e manipulação psicológica para enganar as vítimas e obter informações confidenciais ou sensíveis por meio de uma ligação telefónica. Neste tipo de ataque, os criminosos fazem-se passar por indivíduos ou organizações confiáveis, como bancos, empresas de serviços, órgãos governamentais ou até mesmo colegas de trabalho, com recurso a números de telefone falsos ou técnicas de falsificação de identificação de chamada para que esta assemelhe-se a uma fonte legítima;

tt) **Vulnerabilidade:** uma fraqueza, susceptibilidade ou falha num sistema que um atacante pode aceder e explorar para comprometer a segurança dum sistema, tendo origem da confluência de três elementos: a existência duma susceptibilidade ou falha num sistema; o acesso por um atacante à essa falha e a capacidade do atacante explorar a falha.

Preço — 80,00 MT

IMPRENSA NACIONAL DE MOÇAMBIQUE, E.P.