**Aviso nº. /GBM/2022**

**Maputo, Novembro, 2022**

|  |  |
| --- | --- |
| **Assunto:** | **Directrizes de Gestão do Risco e Resiliência Cibernética** |

 Os ataques cibernéticos têm vindo a aumentar em frequência, sofisticação e impacto, com os perpetradores a refinar, continuamente, os seus esforços para comprometer sistemas, redes e informação em todo o mundo. O sector financeiro, dada a crescente e indispensável utilização da tecnologia, é um dos alvos mais proeminentes de tais ataques, pelo que se impõe o estabelecimento de directrizes para a mitigação do risco.

Nestes termos, 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 na data da sua publicação.

 As dúvidas na interpretação e aplicação do presente Aviso são esclarecidas pelo Departamento de Supervisão Prudencial.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Rogério Lucas Zandamela**

**Governador**

### DIRECTRIZES DE GESTÃO DO RISCO E RESILIÊNCIA CIBERNÉTICA

# CAPITULO I

### DISPOSIÇÕES GERAIS

### Artigo 1

### Objecto

As presentes Directrizes estabelecem o quadro geral de governação, gestão do risco e resiliência cibernética, segundo o qual as instituições de crédito e sociedades financeiras devem adaptar às suas necessidades e tecnologias específicas, tomando em consideração o princípio da proporcionalidade.

### Artigo 2

### Objectivos

As presentes Directrizes têm como objectivo:

1. promover a governação e gestão do risco cibernético no sector financeiro;
2. estabelecer os requisitos para as instituições aperfeiçoarem a sua postura no que diz respeito à resiliência cibernética.

### Artigo 3

### Âmbito de Aplicação

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

**Artigo 4**

**Auto-avaliação do risco cibernético**

1. As instituições devem realizar a auto-avaliação do risco cibernético e remeter os respectivos resultados ao Banco de Moçambique, bem como o Plano de Remediação para a mitigação dos riscos, nos termos das presentes Directrizes.
2. Os documentos referidos no número anterior devem ser remetidos ao Banco de Moçambique no prazo de 90 dias, contados a partir da data de publicação do presente Aviso e, subsequentemente, até ao dia 30 de Junho de cada ano.

**Artigo 5**

**Reporte de Incidentes**

As instituições devem reportar os incidentes cibernéticos no prazo máximo de 48 horas, contadas do momento da sua ocorrência, pela via e no modelo determinados pelo Banco de Moçambique.

# CAPITULO II

**COMPONENTES DE GESTÃO DO RISCO CIBERNÉTICO**

**Secção I**

**Gestão do Risco Cibernético**

**Artigo 6**

**Componentes de gestão**

1. A Gestão do Risco Cibernético contempla 9 (nove) componentes, designadamente:
2. Governação;
3. Identificação;
4. Protecção;
5. Detecção;
6. Resposta e recuperação;
7. Consciência situacional;
8. Teste;
9. Terceirização (*outsourcing*);
10. Aprendizagem e evolução.
11. Para efeitos do presente Aviso, entende-se por:
12. **Governação:** mecanismos implementados pelas instituições com o objectivo de viabilizar o estabelecimento, implementação e revisão da abordagem de gestão do risco cibernético;
13. **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, de modo a direccionar, de forma efectiva, os seus esforços na detecção, resposta e recuperação à cada uma daquelas funções;
14. **Protecção**: conjunto de controlos, sistemas e processos de segurança que as instituições implementam para proteger a confidencialidade, integridade e disponibilidade da informação. As medidas de protecção devem ser proporcionais ao ambiente de ameaça e à exposição da instituição ao risco cibernético;
15. **Detecção**: conjunto de medidas que permite às instituições reconhecer sinais de potenciais incidentes cibernéticos ou detectar intrusões ocorridas. A detecção tempestiva deve assegurar que as instituições tenham um tempo apropriado para implementar medidas adequadas contra potenciais intrusões e permitir a contenção proactiva das intrusões em curso;
16. **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. 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;
17. **Consciência Situacional**: práticas que permitem às instituições compreenderem o ambiente de ameaças cibernéticas em que operam, as implicações de estar nesse ambiente para seus negócios e a adequação de suas medidas de mitigação de riscos cibernéticos. As práticas permitem a construção de um forte nível de consciencialização e compromisso para assegurar a resiliência cibernética global;
18. **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;
19. **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 considere o risco cibernético associado e o risco decorrente da interligação do ecossistema financeiro;
20. **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 tornar-se eficaz no acompanhamento da rápida evolução das ameaças cibernéticas.

**Subsecção I**

**Governação**

**Artigo 7**

**Estratégia e *framework***

1. As instituições devem estabelecer uma estratégia e um *framework* de segurança cibernética adaptados à sua natureza, dimensão, perfil de risco e cultura.
2. A estratégia e o *framework* de segurança cibernética têm como finalidade 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 informados por normas nacionais do sector e boas práticas internacionais.

**Artigo 8**

**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 representado por pessoas, processos, tecnologia e dados subjacentes que suportam cada função, actividades, produtos e serviços identificados.
2. As instituições devem identificar e avaliar a existência e eficácia dos controlos de protecção contra o risco identificado, com vista a apurar o risco residual.
3. 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.
4. As instituições devem adoptar uma abordagem baseada no risco na aplicação das Directrizes e projectar os esforços de mitigação por forma que as medidas a implementar sejam proporcionais ao seu nível de exposição ao risco cibernético.

**Artigo 9**

**Papéis e responsabilidades**

1. As instituições devem definir papéis e responsabilidades com o objectivo de:
	* + 1. 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 a fiscalização do risco cibernético;
			2. 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;
			3. Garantir que seja estabelecida uma função de segurança de informação com recursos adequados, autoridade apropriada e que tenha acesso ao órgão da administração, sempre que aplicável; e
			4. Salvaguardar que a governação e fiscalização da função de segurança da informação seja independente das operações, por forma a assegurar uma adequada segregação de funções e evitar quaisquer potenciais conflitos de interesses.
2. A função referida na alínea c) do número anterior deve ser responsável pela temática cibernética e de segurança da informação dentro da instituição.

**Artigo 10**

**Estratégia de segurança cibernética**

1. As instituições devem estabelecer e manter uma estratégia de segurança cibernética aprovada pelo órgão da administração e alinhadas com as suas estratégias globais.
2. A estratégia de segurança cibernética deve compreender:
3. A importância da resiliência cibernética para a instituição;
4. Os requisitos de alto nível das partes interessadas;
5. A visão e missão relativamente à resiliência cibernética;
6. Os objectivos da resiliência cibernética;
7. O apetite ao risco cibernético;
8. As metas de resiliência cibernética e o respectivo plano de implementação;
9. O âmbito de alto nível da tecnologia e dos activos utilizados para gerir a resiliência cibernética;
10. O modo como iniciativas de resiliência cibernética são entregues, geridas e financiadas;
11. A integração da resiliência cibernética em pessoas, processos, tecnologia e iniciativas institucionais novas ou já existentes.
12. 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 11**

***Framework* de segurança cibernética**

1. O *framework* de segurança cibernética deve:

* + - 1. Incorporar, no mínimo, as seguintes áreas:
1. Identificação, incluindo a classificação e risco de activos;
2. Protecção, incluindo os controlos lógicos e físicos;
3. Segurança de recursos humanos;
4. Gestão de alterações e *patches*;
5. Gestão de segurança de terceiros;
6. Detecção;
7. Incidentes de segurança eforense digital;
8. Resposta e recuperação;
9. Testes;
10. Consciência situacional;
	* + 1. Definir como as instituições estabelecem a sua tolerância ao risco e objectivos cibernéticos e como identificam, mitigam e gerem o seu risco cibernético;
			2. Incorporar as directrizes do presente Aviso relacionadas com a governação, capacitação e gestão de riscos de terceiros;
			3. Ser elaborado, tendo em conta os componentes referidos no artigo 6 do presente Aviso, e estar alinhado às normas (*standards*) e boas práticas internacionais orientadas para o sector financeiro;
			4. Ser consistente com o *framework* organizacional de gestão de risco;
			5. 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;
			6. Articular, claramente, a forma como as instituições identificam o risco cibernético e determinar os controlos necessários para manter o risco dentro do apetite estabelecido.

**Artigo 12**

**Políticas, normas e procedimentos de segurança cibernética**

1. As instituições devem estabelecer políticas, normas e procedimentos de segurança cibernética orientados pelas presentes Directrizes, por *standards* e boas práticas internacionais, por forma a gerir os seus riscos cibernéticos e salvaguardar os activos de informação, tendo em consideração a evolução tecnológica e o panorama das ameaças cibernéticas.

2. 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 ao apetite de risco organizacional.

3. 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:

1. Assegurar que as instituições cumpram os requisitos estabelecidos nas presentes Directrizes;
2. 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:

* + - 1. Assegurar, em coordenação com órgãos da gestão de topo, o estabelecimento de uma estratégia e *framework* de segurança cibernética sólidos e robustos, devidamente implementados e mantidos;
			2. Exigir à gestão de topo que colabore com as outras partes interessadas, conforme relevante e apropriado, a fim de assegurar a resiliência cibernética sistémica;
			3. Assegurar que as funções e responsabilidades referentes à segurança estejam claramente definidas no contrato ou no Acordo de Nível de Serviço (*Service Level Agreements – SLA*) com prestadores de serviços terceirizados; e
			4. Assegurar a realização da auto-avaliação do risco cibernético.

**Artigo 14**

**Responsabilidades da gestão de topo**

1. O órgão de administração e a gestão de topo deve garantir que um executivo sénior (por exemplo, o *Chief Information Security Officer* – *CISO*) seja responsável pela implementação da estratégia e estrutura de resiliência cibernética a 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 e sobre questões-chave.
3. O executivo sénior referido no nº 1 do presente artigo deve ser independente, possuir adequadas competências, conhecimento, experiência, ter recursos suficientes e acesso directo ao órgão de administração.

 **Subsecção II**

 **Identificação**

**Artigo 15**

**Deveres**

1. As instituições devem:

1. 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;
2. 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, resposta e esforços;
3. Realizar 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;
4. Manter um inventário actualizado, pelo menos, anualmente, de todas as funções críticas, funções-chave, processos, activos de informação, fornecedores de serviços de terceiros e interligações;
5. 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;
6. 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;
7. 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;
8. 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;
9. Criar e manter um mapa de redes, contendo a relação dos recursos de rede com um plano de endereçamento de IP (*Internet Protocols*) que localizam dispositivos de roteamento e servidores que suportam as funções críticas e que identificam ligações com o mundo exterior.

2. O mapa referido na alínea i) do número anterior deve ser actualizado, sempre que se mostre necessário.

**Subsecção III**

**Protecção**

**Artigo 16**

**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 17**

 **Objectivos de segurança**

1. As instituições devem implementar um conjunto abrangente e apropriado de controlos de segurança que permitam alcançar os objectivos de segurança, 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 devem assegurar:
3. 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;
4. A protecção, integridade, confidencialidade e disponibilidade dos dados em estado de armazenamento, utilização e trânsito;
5. A conformidade com as leis, regulamentos e normas aplicáveis.
6. As instituições devem actualizar, pelo menos, anualmente, os seus controlos de segurança, 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 18**

**Monitorização de sistemas**

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

1. Todas as actualizações disponíveis sejam instaladas de forma atempada e segura, sendo mantidas, adequadamente, com o devido suporte;
2. São implementadas e testadas camadas adicionais de segurança, onde são identificadas vulnerabilidades nos sistemas;
3. São descartados e substituídos todos os sistemas legados 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 19**

**Gestão de acessos**

1. As instituições devem garantir a gestão adequada de acessos, assegurando:
2. 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;
3. A implementação de controlos que limitam e monitoram, de forma rigorosa, o pessoal com maior nível de privilégio ou direitos de acesso;
4. A criação de processos com vista a monitorizar o acesso ao sistema e à informação e accionar alertas em caso de tentativas de acesso não autorizado;
5. Que o acesso aos activos de informação e instalações associadas são geridos de forma proporcional ao risco avaliado de acesso não autorizado;
6. O estabelecimento de mecanismos de gestão de identidade e de controlo de acesso**,** por forma a proporcionar uma administração eficaz e consistente dos utilizadores, responsabilização e autenticação, de modo a:
	1. Implementar políticas e procedimentos de segurança e controlo de acesso;
	2. 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;
	3. 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;
	4. Sujeitar os prestadores de serviços e terceiros com acesso aos activos de informação à mesma monitorização e restrições de acesso concedida aos seus colaboradores;
	5. 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;
	6. 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.
	7. Implementar rastreios (*screening*) e verificações de antecedentes baseados no risco para todos os novos colaboradores e terceiros, antes da sua contratação;
	8. Assegurar que os colaboradores em posições sensíveis, por exemplo, aqueles que mudam para funções que requerem acesso privilegiado a sistemas críticos ou que se tornam pessoal de alto risco, sejam pré-seleccionados.
7. Ao pessoal com maior privilégio ou funções de administrador de sistemas/redes, referido na alínea b) do n.º 1 do presente artigo, devem ser fornecidas formações e treinamentos personalizados, atendendo às suas atribuições e ao significativo nível de risco cibernético a que estão expostos.

**Artigo 20**

**Gestão de alterações**

* + - 1. As instituições devem possuir políticas, procedimentos e controlos para a gestão de alterações que:
1. Incluam critérios de prioridade e classificação das alterações (por exemplo, alteração normal *vs.* alteração de emergência);
2. Permitam que antes de qualquer alteração, as instituições assegurem que o pedido de alteração é:
3. Revisto, a fim de satisfazer as necessidades de negócio;
4. categorizado e avaliado por forma a identificar potenciais riscos e assegurar que não têm um impacto negativo na confidencialidade, integridade, disponibilidade e nos sistemas e dados da instituição;
5. aprovado antes de ser implementado pelo nível de gestão adequado.
6. Certifiquem que a equipa de segurança cibernética é envolvida ao longo do ciclo de vida do processo de gestão de alterações.
	* + 1. As instituições devem testar, validar e documentar as alterações aos sistemas de informação antes da sua implementação em produção, podendo incluir testes de integração, testes de não regressão e testes de aceitação pelo utilizador, entre outros.
			2. As alterações aos sistemas de informação incluem, mas não se limitam, a modificação de componentes de *hardware, software* ou *firmware* e definições de configuração do sistema e de segurança.
			3. 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 21**

 **Gestão de *patches***

1. As instituições devem ter uma política e processos abrangentes de gestão de *patches* que incluam:
2. A identificação de *patches* apropriados para sistemas específicos e analisar os impactos, se instalados;
3. Regras que assegurem que os *patches* sejam instalados correctamente (por exemplo, aplicando o princípio dos quatro olhos) e testados antes e monitorados após a instalação;
4. A documentação de todos os procedimentos associados, como configurações específicas exigidas.
5. As instituições devem considerar o uso de configuração de base (*standard*) de recursos de TI, de modo a facilitar o processo de gestão de *patches.*
6. As instituições devem assegurar que as instalações de novos *patches* tenham a aprovação prévia do nível de gestão adequado.

**Artigo 22**

**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 23**

 **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 24**

**Controlos de segurança de dados**

1. As instituições devem implementar controlos de segurança de dados que permitam:
2. Desenvolver uma política global de prevenção de perda de dados e adopção de medidas para detectar e evitar o acesso não autorizado, modificação, cópia ou transmissão dos dados sensíveis em trânsito, armazenados ou em utilização;
3. Proteger os dispositivos terminais, através da implementação de medidas apropriadas para prevenir e detectar o furto de dados e modificações não autorizadas;
4. 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 implementados a nível da instituição;
5. Certificar que os dados sensíveis armazenados em sistemas e dispositivos terminais são codificados e protegidos por fortes mecanismos de controlo de acesso;
6. Salvaguardar que apenas os sistemas informáticos autorizados, dispositivos terminais e meios de armazenamento de dados são utilizados para comunicar, transferir ou armazenar dados sensíveis;
7. Implementar controlos de segurança para prevenir e detectar a utilização de serviços de *Internet* não autorizados que permitam aos utilizadores comunicar ou armazenar dados sensíveis;
8. Assegurar que a utilização de dados de produção sensíveis em ambientes não produtivos é restringida;
9. Salvaguardar que os dados sensíveis são permanentemente apagados dos meios de armazenamento, sistemas informáticos e dispositivos terminais, antes de serem eliminados ou redistribuídos;
10. 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 impossibilitada, são previstos mecanismos que permitam a destruição segura dos suportes de armazenamento que contenham informação da instituição;
11. Estabelecer acordos de não-divulgação ou de confidencialidade com os utilizadores.
12. Em situações excepcionais, caso os dados de produção referidos na alínea g) do número anterior são 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 25**

**Controlos de segurança de aplicações e sistemas**

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

1. Implementar uma abordagem de segurança por projecto referente à incorporação de controlos de segurança em cada fase do desenvolvimento de aplicações, a fim de minimizar as vulnerabilidades do sistema e reduzir as possibilidades de ataque;
2. Determinar o nível aceitável de segurança necessário para satisfazer as necessidades de negócio e avaliar as potenciais ameaças e riscos relacionados com o sistema;
3. Assegurar que os requisitos de segurança relativos ao controlo de acesso ao sistema, autenticação, autorização de transacção, integridade dos dados trilhas de auditoria, monitorização dos eventos de segurança e tratamento de excepções são, claramente, especificados nas fases iniciais de desenvolvimento ou aquisição do sistema;
4. 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 26**

 **Controlos de segurança de rede**

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

1. Instalação de dispositivos de segurança de rede para proteger a rede, entre a elas e *Internet* e as ligações com prestadores de serviços;
2. Implantação de sistemas de detecção ou prevenção de intrusão na rede para detectar e bloquear o tráfego malicioso;
3. Revisão da arquitectura de rede, incluindo a concepção da sua segurança e das respectivas interligações numa base periódica, de modo a identificar potenciais vulnerabilidades;
4. Implementação de controlos de acesso à rede para detectar e impossibilitar a ligação de dispositivos não autorizados à sua rede;
5. 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 por exemplo, terminais de pagamento SWIFT;
6. Encriptação das ligações remotas, de modo a prevenir fugas de dados, através de ataques como os relacionados com a varredura de rede (exemplo: *network sniffing* e *eavesdropping*).

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

**Artigo 27**

**Criptografia**

1. As instituições devem implementar a criptografia baseada no seguinte:
2. Estabelecimento de políticas, normas e procedimentos de gestão de chaves criptográficas abrangendo a geração, distribuição, instalação, renovação, revogação, recuperação e expiração de chaves;
3. Adopção de algoritmos criptográficos a partir de normas internacionais estabelecidas;
4. Garantia de que as chaves criptográficas são geradas com segurança e protegidas contra divulgação não autorizada em sistemas reforçados e são resistentes a adulterações;
5. Utilização de um método seguro de destruição de chaves, por forma a assegurar que não são recuperáveis quando expiradas ou revogadas;
6. Determinação da duração de vida apropriada de cada chave criptográfica, com base em factores, como:
7. a sensibilidade dos dados;
8. a criticidade do sistema a ser protegido;
9. as ameaças e riscos a que os dados ou sistema podem estar expostos;
10. Manuntenção das 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;
11. Garantia de 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.
12. 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.
13. A chave criptográfica referida na da alínea e) do nº 1 do presente artigo deve ser substituída com segurança, antes de expirar no final da sua vida útil.

**Subsecção IV**

**Detecção**

 **Artigo** 28

 **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 que atinjam um nível de maturidade aceitável devem definir, considerar e documentar o perfil de base das actividades do sistema para auxiliar na detecção de prováveis desvios, como, por exemplo, 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. A classificação nível de maturidade aceitável, referido no nº 2 do presente artigo, é estabelecida por Circular do Banco de Moçambique.

**Artigo 29**

**Monitorização das actividades dos sistemas informáticos**

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

**Artigo 30**

**Monitorização e análise contínua**

1. As instituições devem estabelecer um sistema de monitorização e análise contínua de eventos cibernéticos, como por exemplo, através de Centro de Operações de Segurança – SOC ou equivalente e a detecção e rápida resposta a incidentes cibernéticos.
2. As instituições devem definir processos, papéis e responsabilidades para as operações de segurança.
3. As instituições devem estabelecer um processo de recolha, revisão e retenção de *logs* dos sistemas, de modo a facilitar as operações de monitorização de segurança.
4. Os registos decorrentes do processo referido no número anterior devem ser protegidos contra o acesso não autorizado.
5. As instituições devem 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.
6. As instituições devem assegurar que as suas capacidades de detecção e monitorização permitem a recolha de informação suficiente para apoiar a investigação forense de eventos e incidentes cibernéticos.

**Artigo 31**

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

**Artigo 32**

**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 33**

**Camadas de controlo**

* + - 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.

**Subsecção V**

**Resposta e recuperação**

**Artigo 34**

**Mecanismos de resposta**

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

**Artigo 35**

**Políticas e processos de gestão de incidentes**

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

1. Aprimorar a resiliência;
2. Assegurar a continuidade do negócio,
3. Melhorar a confiança dos clientes e de partes interessadas;
4. Potencialmente, reduzir qualquer impacto.

**Artigo 36**

**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, por exemplo,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 37**

**Estratégia de comunicação**

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

**Artigo 38**

**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 39**

**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 (*fallback*) associado, quando aplicável.

**Artigo 40**

**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 41**

**Processos de resposta e recuperação**

As instituições devem:

1. Dispor de processos de resposta, retomada, recuperação e ambientes de simulação de incidentes cibernéticos integrados com a gestão de crises, continuidade do negócio, planeamento da recuperação de desastres e operações de recuperação;
2. Implementar processos e 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;
3. Ter processos e procedimentos implementados 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.

**Subsecção VI**

**Consciencialização situacional**

**Artigo 42**

**Cultura de consciencialização**

1. As instituições devem promover uma culturainstitucional 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 um alto nível de consciencialização e compromisso para a resiliência cibernética.

**Artigo 43**

**Formação**

1. As instituições devem assegurar:
2. A existência de um programa de formação contínua e testes de consciencialização sobre o risco e resiliência cibernética para todo o pessoal;
3. O equilíbrio adequado de competências, conhecimentos e experiência para compreender e avaliar os riscos cibernéticos que enfrentam.
4. As instituições devem elaborar programas de consciencialização e educação do cliente em matérias de literacia e inclusão financeira, de modo a dotar os seus clientes de técnicas de detecção de comunicações fraudulentas.

**Artigo 44**

**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 cibernéticas.

**Artigo 45**

 **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 TI, 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:
3. *Logs* de aplicações, sistemas e redes;
4. Dispositivos de segurança, tais como *firewalls* e Sistemas de Detecção de Intrusões (*Intrusion Detection Systems*-IDS);
5. Fornecedores fiáveis de informações sobre ameaças;
6. Informação pública disponível.

**Artigo 46**

**Análise da informação**

As instituições devem analisar toda a informação recolhida para gerar um entendimento relevante sobre ameaças cibernéticas e 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 47**

**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 48**

**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.

**Artigo 49**

**Canais de comunicação**

1. As instituições devem estabelecer canais de comunicação directos, fiáveis e seguros com as partes interessadas, para a troca de informação.
2. As instituições devem estabelecer mecanismos padronizados de comunicação com os seus clientes, em caso de ataques cibernéticos dedicados a este grupo (exemplo: 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 (por exemplo, a exclusão de *links* clicáveis nas comunicações da instituição).

**Subsecção VII**

**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 estão implementados correctamente, se funcionam como pretendido e se 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:
1. Ritmo que as vulnerabilidades e ameaças mudam;
2. Criticidade e sensibilidade do sistema informático ou da informação;
3. Consequências de um incidente de segurança;
4. Riscos associados à exposição a ambientes em que as instituições são incapazes de aplicar as suas políticas de segurança;
5. Materialidade e frequência das alterações aos activos de informação.
	* + 1. 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 (terceiros).

**Artigo 52**

**Tipos de testes**

* + - 1. Com base no princípio da proporcionalidade, dependendo do perfil de risco, dimensão, estrutura de governação, ambiente operativo, complexidade, sofisticação de produtos e serviços e interligação com outras entidades, as instituições devem realizar os seguintes testes:
1. Avaliações de vulnerabilidades;
2. Testes baseados em cenários;
3. Testes de intrusão;
4. Testes de *red team*.
	* + 1. 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**

As instituições devem assegurar que a garantia do controlo de segurança é fornecida por pessoal devidamente qualificado.

**Artigo 55**

**Avaliações de Vulnerabilidades**

As instituições devem:

1. Estabelecer um processo de realização de avaliações, pelo menos, trimestralmente, de vulnerabilidades nos seus sistemas informáticos, para identificar vulnerabilidades de segurança e assegurar que os riscos decorrentes dessas vulnerabilidades são tratados atempadamente;
2. Assegurar que a frequência das avaliações de vulnerabilidades é proporcional à criticidade dos sistemas informáticos e aos riscos de segurança que aquele estão expostos.

**Artigo 56**

**Testes Baseados em Cenários**

1. As instituições devem:
2. Realizar exercícios, com periodicidade anual, de simulação baseados em cenários, para validar as suas capacidades de resposta e recuperação, bem como os seus planos de comunicação, contra as ameaças cibernéticas prevalecentes;
3. Conceber o exercício de simulação baseado em cenários, utilizando informação de ameaça que seja relevante para o seu ambiente de negócio, a fim de identificar:
4. os agentes mais susceptíveis de representar uma ameaça;
5. as tácticas, técnicas e procedimentos mais susceptíveis de serem utilizados em tais ataques.
6. O exercício deve incluir, mas não se limitar, à de simulação de ataque e defesa.

**Artigo 57**

**Testes de Intrusão**

As instituições devem:

1. Realizar testes de intrusão para obter uma avaliação aprofundada das suas defesas de segurança cibernética;
2. Realizar uma combinação de testes de *black box, grey box and white box* para sistemas informáticos e activos de informação;
3. Assegurar que a frequência dos testes de intrusão é determinada com base em factores como a criticidade e a exposição a riscos cibernéticos;
4. Realizar testes de intrusão 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.

**Artigo 58**

**Testes de *Red Teaming***

1. Com base no princípio da proporcionalidade e tendo implementado com sucesso as medidas que mitigam devidamente as deficiências detectadas através das avaliações de vulnerabilidade, testes baseados em cenários e testes de intrusão, as instituições sistémicas devem:
2. Realizar exercícios independentes de *Red Teaming*, pelo menos anualmente, tais como:
3. execução de ataques controlados de engenharia social;
4. plantação de dispositivos.
5. Desafiar as funções críticas sobre possíveis vulnerabilidades e a eficácia de controlos de mitigação, incluindo o seu pessoal, processos e tecnologia.
6. A *Red Team* deve testar a forma como a equipa de segurança da instituição responde às várias ameaças.
7. 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.
8. As instituições sistémicas e com um nível aceitável de maturidade de segurança cibernética devem realizar o teste de TLPT (*Threat Led Penetration Testing*), tendo em atenção os critérios definidos pelo Banco de Moçambique em instrumento específico.
9. Em função do risco, o Banco de Moçambique pode solicitar a realização do teste TLPT às instituições que não tenham ainda atingindo os pressupostos referidos no número anterior.
10. O teste referido no nº 4 deve ser conduzido por entidades com certificações acreditadas e independentes das instituições.

**Artigo 59**

**Controlos de gestão de remediação**

1. Após a realização dos testes ou exercício de segurança cibernética, as instituições devem estabelecer controlos de gestão de remediação com o objectivo de:
2. 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;
3. 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;
4. 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.
5. O processo referido na alínea a) do número anterior deve, no mínimo, incluir:
6. Avaliações da gravidade e a classificação dos problemas;
7. Prazos para remediar os problemas de gravidade diferente;
8. Avaliações de risco, sempre que necessário;
9. Estratégias de mitigação para gerir desvios do *framework* de segurança cibernética.

**Subsecção VIII**

**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 seus resultados 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 obter relatórios de auditoria conjunta de fornecedores que suportam funções críticas, como formas de garantias quanto à postura de segurança do seu prestador de serviços de terceiros.
3. A auditoria conjunta mencionada no número anterior pode ser organizada por grupos de instituições que partilhem um ou mais fornecedores de serviços ou sejam facilitadas por estes, podendo ser realizadas por representantes das instituições participantes ou por especialistas nomeados em seu nome.
4. Nos casos em que as auditorias conjuntas conduzam a conclusões comuns e partilhadas, cada instituição participante deve avaliar, individualmente, o contexto e abrangência das conclusões no seu ambiente.

**Artigo 62**

**Contratação de terceiros**

As instituições devem utilizar contratos com terceiros para impor princípios de segurança cibernética que sejam proporcionais ao seu apetite ao risco cibernético devendo incluir:

1. Papéis e responsabilidades de cada parte envolvida relativamente ao acesso aos dados;
2. Resposta e comunicação de incidentes;
3. Planeamento da continuidade do negócio;
4. Cessação;
5. Portabilidade dos dados;
6. Direitos de auditoria e acesso a relatórios de certificação.

**Artigo 63**

**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 64**

**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 65**

**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, trimestralmente.

**Artigo 66**

**Deveres**

Para além dos deveres indicados na presente Subsecção, as instituições devem:

1. Conceber e verificar os controlos de segurança para detectar e prevenir possíveis intrusões decorrentes de ligações de terceiros;
2. 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;
3. Integrar no seu plano de resposta terceiros que prestam serviços para as suas funções críticas;
4. Avaliar a substituibilidade dos terceiros que prestam serviços para as suas funções críticas e incluir, no seu plano de continuidade de negócios, a transição para prestadores de serviços alternativos ou a realização de serviços críticos internamente que seja compatível com a criticidade e seu apetite ao risco.

**Subsecção IX**

**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 interessadarelevante, 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, mas não se limitam, indicadores, os seguintes:
3. Percentagem do pessoal que recebeu formação em segurança cibernética;
4. Percentagem de incidentes reportados dentro do prazo exigido por categoria;
5. Percentagem de vulnerabilidades mitigadas dentro de um período de tempo definido após a descoberta;
6. relatórios anuais de monitorização do progresso dos indicadores.

# Glossário

|  |  |
| --- | --- |
|  **Abordagem baseada no risco** | A 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. |
| **Activo de informação** | Qualquer porção de dados, dispositivos ou outros componentes do ambiente que suporta actividades relacionadas com a informação, incluíndo dados, *hardware* e *software*. Os activos de informação não estão limitados apenas àqueles detidos pela instituição, incluindo, também, àqueles que são alugados ou contratados e aqueles que são utilizados pelos provedores de serviços para fornecerem os seus serviços. |
| **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. |
| **Ataque cibernético** | O uso de uma vulnerabilidade por um adversário para obter vantagem de uma ou mais fraquezas com o intuito de infligir um efeito adverso no ambiente de TIC. |
| **Auditoria Conjunta (*pooled audit*)** | Auditorias combinadas mais eficientes e rentáveis para as instituições e menos incómoda para os fornecedores de serviços que gerem ambientes com múltiplas instâncias, onde um serviço serve à grupos distintos de clientes.  |
| **Centro de operações de segurança (SOC)** | Uma função ou serviço responsável pela monitorização, detecção e contenção de incidentes. |
| **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. |
| **Detecção** | Desenvolvimento e implementação de actividades apropriadas visando a identificação da ocorrência de eventos cibernéticos. |
| **Disponibilidade** | A propriedade de ser acessível e utilizável como esperado quando necessário. |
| **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, etc. |
| **Estratégia de resiliência cibernética** | Princípio de alto nível e planos a médio prazo das instituições para alcançarem os seus objectivos de gestão do risco cibernético. |
| **Evento cibernético** | Uma ocorrência observável num sistema de informação ou rede. |
| **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. |
| **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. |
| **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. |
| **Incidente cibernético** | Evento com um impacto adverso real na segurança das redes e dos sistemas de informação |
| **Indicador** | Uma ocorrência ou sinal que revele que um incidente ocorreu ou está em curso. |
| **Indicadores de Risco** | Estatísticas ou matrizes que podem fornecer a posição do risco da instituição, podendo incluir o volume e/ou frequência das violações da lei, a frequência das reclamações, número de processos judiciais e frequência de fraudes, reais ou suspeitas, ou actividades de branqueamento de capitais e podem ainda fornecer ainda bons incentivos, indexando o risco ao capital necessário para melhoria desejável no cumprimento da função. |
| **Integridade** | Relativamente a informação, um sistema de informação ou um componente dum sistema, é a propriedade de não ter sido modificado ou destruído de forma autorizada. |
| **Investigação *forense*** | A aplicação de técnicas investigativas e analíticas para a obtenção e preservação de evidências de dispositivos digitais impactados por ataques cibernéticos. |
|  |  |
| **Órgão de administração** | Órgão que detém a responsabilidade, em última instância, de avaliar as opções estratégicas, orientar a gestão de topo e monitorizar o rumo estratégico da instituição, cabendo-lhe definir e aprovar o apetite ao risco, as estratégias globais do negócio, as políticas que orientam a tomada e gestão de riscos na instituição e assegurar que a gestão de topo é plenamente capaz de gerir as actividades que a instituição desenvolve dentro dos limites do apetite ao risco que aprovou. |
| **Padrões, directrizes e práticas internacionalmente aceites** | Normas, directrizes e práticas que reflectem as melhores abordagens da indústria para a gestão das ameaças cibernéticas e incorporam as soluções de resiliência cibernética globalmente recomendadas como as mais efectivas. |
| **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. |
| ***Patches***  | Actualizações ou correcções de *software* fornecidas pelo provedor da aplicação, por forma a melhorar o uso ou *performance*. |
| **Perfil de risco cibernético** | O risco cibernético assumido e mensurado num determinado momento. |
| ***Phishing*** | Ameaça que consiste em mensagens falsas enviadas por criminosos que se fazem passar por empresas ou pessoas confiáveis. As [mensagens encapsulam tácticas de engenharia social](https://www.metacompliance.com/pt/blog/phishing-and-ransomware/elements-convincing-phishing-attack), aplicando o fingimento, a confiança e o desejo de clicar para encorajar os destinatários a divulgar informações pessoais, tais como palavras-passe e detalhes de cartões de crédito, sendo a forma mais comum de ataque com recurso a *e-mails*. |
| **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. |
| **Processos e procedimentos** | Descrição de um conjunto organizado de práticas e actividades específicas necessárias para o alcance de certos objectivos e produzir um conjunto de resultados que suportam o alcance das metas do negócio como um todo. |
| **Programa de gestão do risco** | Descrição formal do sistema de governação e processos de gestão de riscos estabelecidos na instituição.  |
| **Protecção** | Desenvolvimento e implementação das salvaguardas, controlos e medidas apropriadas visando garantir a provisão de serviços de infra-estruturas críticas. |
| ***Smishing*** | Variante do *phishing* que ocorre por SMS (mensagens de texto recebidas no celular), onde os criminosos se fazem passar por empresas conhecidas oferecendo prémios que não existem, por instituições bancárias solicitando actualização de cadastro ou por lojas com promoções, cujo objectivo é d aliciar a vitima a clicar num *link* que pode tanto levá-lo a uma página falsa que pedirá seus dados quanto infectar seu dispositivo. |
| ***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. |
| ***Trilhas de Auditoria*** | Também chamada de *log* de auditoria, são usadas para assegurar o fluxo preciso das transações num sistema e fornecem um histórico de mudanças ocorridas em objectos no sistema. |
| ***Vishing*** | Variante do *phishing*, que ocorre por voz quando os criminosos ligam para o telefone da vítima e se fazem passar por uma empresa ou algum desconhecido, solicitando dados ou a instalação em algo no dispositivo electrónico da vítima. Geralmente, são pessoas bem articuladas e convincentes, que já possuem algum tipo de informação prévia e básica sobre a vitima.  |

|  |  |
| --- | --- |
| ***Framework* de resiliência 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. |
| **Recuperação** | A restauração de quaisquer funcionalidades ou serviços afectados devido a eventos cibernéticos. |
| ***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. |
| **Resposta** | A capacidade da instituição desenvolver e implementar as actividades apropriadas para estar capaz de tomar as devidas acções quando detectados eventos cibernéticos. |
| **Resiliência cibernética** | A capacidade das instituições para antecipar, aguentar, conter e rapidamente recuperar de um ataque cibernético. |
| **Restauração** | O reinício das funções após a ocorrência dum incidente cibernético, deve a instituição 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 e ser desenhado para garantir que os sistemas críticos de TIC podem restaurar as operações dentro de duas horas após eventos disruptivos. |
| **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. |
| **Tolerância ao risco** | A quantidade e tipo de risco que uma instituição está disposta a aceitar para alcançar os seus objectivos estratégicos (pode também ser referida como “apetite de risco”). |
| **Tolerância ao risco cibernético** | A probabilidade de incorrer no risco cibernético, constituindo o nível de risco que uma instituição tenciona assumir no alcance dos seus objectivos estratégicos. |
| **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. |

## Apêndice A: Lista de Acrónimos

|  |  |
| --- | --- |
| **IDS** | *Intrusion Detection System* |
| **IP** | *Internet Protocol* |
| **TIC** | Tecnologias de Informação e Comunicações |
| **TLPT** | *Threat Led Penetration Test* |
| **RPO** | *Recovery Points Objectives* |
| **RTO** | *Recovery Time Objectives* |
|  |  |
|  |  |