REPÚBLICA DE MOÇAMBIQUE

MINISTÉRIO DAS COMUNICAÇÕES E TRANSFORMAÇÃO DIGITAL

PROPOSTA DE REVISÃO DO REGULAMENTO DE SEGURANÇA DE REDES DE TELECOMUNICAÇÕES

Maputo, Setembro de 2025

Havendo necessidade de alterar as disposições do Regulamento de Segurança de Redes de Telecomunicações, aprovado pelo Decreto n.º 66/2019 de 1 de Agosto, ao abrigo do disposto na alínea c) do artigo 13 e no 42, ambos da Lei das Telecomunicações, o Conselho de Ministros determina:

Artigo 1. São alterados os artigos 2 a 7, 9 a 18 do Regulamento de Segurança de Redes de Telecomunicações, aprovado pelo Decreto n.º 66/2019 de 1 de Agosto, que passam ter a seguinte redacção:

ARTIGO 2

(Objecto)

O presente Regulamento tem por objecto estabelecer procedimentos de execução de medidas a serem observadas em matéria de segurança e integridade da rede e infra-estruturas de telecomunicações, bem como os procedimentos e formato de notificação de incidentes e violações de segurança à Autoridade Reguladora e obrigações de auditoria e fiscalização do cumprimento destas medidas.

ARTIGO 3

(Âmbito)

1. O presente Regulamento é aplicável aos operadores de redes e serviços públicos de telecomunicações **e aos detentores ou gestores de infra-estruturas aptas ao alojamento de redes de telecomunicações, públicas ou privadas, incluindo entidades da Administração Pública, Autarquias Locais, e entidades dos sectores da energia, da água, dos transportes ou outros, públicas ou privadas, que detenham ou explorem tais infra-estruturas.**
2. **O presente Regulamento é igualmente aplicável aos operadores de serviços disponibilizados através da Internet "aberta", incluindo prestadores OTT, exclusivamente no que respeita à segurança e integridade das interfaces e serviços por si disponibilizados e ao seu impacto nas redes estabelecidas no território nacional.**

ARTIGO 4

(Objectivos)

1. …

a) …

b) …

c) …

d) Coordenação com as equipas CSIRT competentes, incluindo a ERIST, para prevenção, detecção e resposta a incidentes.

2. O presente Regulamento aplica-se em articulação com o regime jurídico geral de segurança cibernética, sem prejuízo das obrigações e competências atribuídas às autoridades competentes nos termos desse regime.

ARTIGO 5

(Atribuições da Autoridade Reguladora)

…

a) **Supervisionar, fiscalizar e auditar** a conformidade da segurança das redes de telecomunicações com os padrões internacionais, bem como com as disposições constantes no presente Regulamento;

b) …

c) Coordenar com o CSIRT Nacional e actuar, através da ERIST, como CSIRT sectorial;

d) Aprovar orientações técnicas e modelos de reporte, e determinar a realização de auditorias independentes;

e) Ordenar, quando necessário, o bloqueio de tráfego fraudulento e outras medidas urgentes de mitigação;

f) Promover e coordenar campanhas de formação e sensibilização sobre as matérias previstas neste Regulamento

ARTIGO 6

(Cooperação e partilha de informação)

1. **…**
2. O operador de rede e de serviços públicos de telecomunicações, **em coordenação com a Autoridade Reguladora e a ERIST,** deve criar um serviço de denúncia de potenciais casos de fraude nos serviços de telecomunicações, onde o consumidor pode interagir com o operador.
3. …
4. O operador de rede e de serviços públicos de telecomunicações e a Autoridade Reguladora devem designar um responsável pela segurança e ponto de contacto permanente, **que funcionará como ponto oficial de contacto com o CSIRT Nacional e a ERIST.**
5. **Os operadores devem partilhar com a ERIST, em tempo real, indicadores e alertas relevantes de fraude e segurança, nos termos a definir pela Autoridade Reguladora.**

ARTIGO 7

(Protecção de dados e privacidade)

1. …
2. …
3. …
4. …
5. …
6. …
7. **As disposições do presente artigo relativas às obrigações de protecção de dados e privacidade são aplicáveis, com as necessárias adaptações, à confidencialidade na partilha de informação com a ERIST.**

ARTIGO 9

(Requisitos de segurança)

1. **…**
2. **…**
3. **…**
4. **…**
5. **…**
6. **…**
7. **…**
8. **…**
9. **Sem prejuízo dos números anteriores, a Autoridade Reguladora pode aprovar orientações técnicas complementares, actualizáveis, contendo requisitos detalhados de segurança a observar pelos operadores.**

ARTIGO 10

(Serviço de pagamento móvel)

1. **…**

2. Não sendo possível a separação prevista no número anterior deve ser elevado o nível de mecanismos de segurança, **incluindo mecanismos reforçados de autenticação e segregação de funções.**

ARTIGO 11

(Procedimento de controlo)

…

a) …

b) Avaliar a vulnerabilidade e efectuar teste de penetração, considerando todos os casos de uso de ataques conhecidos para infra-estrutura lógica de telecomunicações em toda a rede de acesso de rádio, rede de transmissão, rede núcleo com comutação de circuitos, rede núcleo com comutação de pacotes, núcleo de pacote evoluído, Subsistema Multimídia IP, Sistemas de Suporte à Operação, Sistemas de Suporte ao Negócio, rede de dados IP/MPLS, entre outros, **incluindo a avaliação da exposição de APIs utilizadas por OTT e interfaces B-PIN/Central de Risco.**

c) …

d) Compilar e actualizar o dossier de segurança, produzir e submeter relatórios anuais ou quando solicitado pela Autoridade Reguladora, depois de acordados os seus termos, **bem como estatísticas de fraude detectada e medidas correctivas implementadas.**

ARTIGO 12

(Procedimentos de gestão de alterações da rede)

1. …

2. …

3. **As alterações com impacto em activos classificados como críticos devem ser notificadas à Autoridade Reguladora com antecedência mínima de 30 dias.**

4. **Após cada alteração relevante, deve ser realizada nova avaliação de risco actualizada e, quando aplicável, testes de integração, de sistemas e de segurança.**

ARTIGO 13

(Sistema de controlo de acessos)

O sistema de controlo de acesso consiste na permissão de acesso de pessoas autorizadas e, para o efeito, o operador de rede e de serviços públicos de telecomunicações deve:

a) Estabelecer e manter Sistemas de Controlo de Acessos físicos e lógicos adequados à prevenção, gestão e redução dos riscos para a segurança e integridade das redes e serviços, tendo em consideração especial os activos constantes do inventário de activos críticos **e devendo os sistemas contemplar, quando aplicável, autenticação multifactor e segregação de funções, e princípio do menor privilégio.**

b) …

c)…

ARTIGO 14

(Sistemas de monitorização e controlo da segurança)

1. …
2. …
3. …
4. …
5. **Os sistemas devem transmitir, em tempo real, alarmes relevantes para a ERIST e articular a resposta com o CSIRT Nacional em incidentes críticos, nos termos definidos pela Autoridade Reguladora.**

ARTIGO 15

(Caracterização geral da segurança)

A caracterização geral da Segurança deve ser assegurada pelos operadores de rede e de serviços de telecomunicações consistindo na elaboração, actualização da sua documentação e deve conter o seguinte:

a) Inventário de activos e activos críticos, com critérios de classificação;

b) Mapa de interfaces expostas (incluindo APIs OTT e integrações B-PIN/Central de Risco);

c) A política de segurança;

d) A informação sobre a abordagem e a metodologia de segurança e de gestão dos riscos adoptadas;

e) A descrição do sistema de gestão de segurança;

f) A descrição das medidas de redundância, de robustez e resiliência da rede;

g) A descrição do Sistema para a Monitorização do Tráfego de Acesso à Internet quando aplicável;

h) A descrição dos Sistemas de Controlo de Acessos;

i) A descrição dos Sistemas de Monitorização e Controlo;

j) A identificação e os contactos do responsável permanente ou alternativo pela Segurança, deve incluir:

i) O nome, designação da função;

ii) O endereço de correio electrónico;

iii) O contacto de telefónico;

iv) O endereço físico do local onde é assegurada a função.

ARTIGO 16

(Plano de segurança)

1. …

2. …

3. …

a) …

b) …

c) …

d) os procedimentos de comunicação ao público e respectivos limiares;

e) o programa anual ou bianual de exercícios de segurança e continuidade, com reporte dos resultados à Autoridade Reguladora.

ARTIGO 17

(Responsável pela segurança)

…

a) …

b) …

c) …

d) Actuar como ponto oficial de contacto com o CSIRT Nacional e a ERIST e assegurar a notificação de incidentes graves em menos de 24 horas.

ARTIGO 18

(Resposta a incidentes de segurança)

A resposta a incidentes de segurança deve ser oferecida por uma unidade e consiste na actuação eficaz, eficiente e preparação contra os riscos, ameaças e vulnerabilidades que afectem os activos críticos na continuidade do funcionamento das suas redes ou de serviços, **incluindo articulação com a ERIST e o CSIRT Nacional, nos termos definidos pela Autoridade Reguladora.**

Glossário

B-PIN – Base de dados pública integrada de numeração centralizada e hospedada na Autoridade Reguladora e que contém todas as Chaves de Identificação dos Subscritores, dados de todos os subscritores, dados de todos os agentes, dados de todos os Dispositivos de Comunicações e dados de todos Módulos de Identificação dos Subscritores nas redes de telecomunicações.

Central de Risco – base de dados centralmente hospedada na Autoridade Reguladora onde constam todos os dados dos Subscritores, Agentes, Módulos de Identificação do Subscritor, Chaves de Identificação dos Subscritores e Dispositivos de Comunicações fraudulentos ou suspeitos de fraudes, e ainda todos dados dos casos de bloqueio e ou impedimentos de uso das redes de telecomunicações.

CSIRT - Equipa Nacional de Resposta a Incidentes de Segurança Cibernética

ERIST – Equipa de Resposta a Incidentes de Segurança nas Redes de Telecomunicações

Activos Críticos – as infra-estruturas, os sistemas de transmissão ou de informação, os equipamentos e os demais recursos, físicos e lógicos, que compõem ou suportam redes de comunicações e respectivos acessos, serviços de comunicações electrónicas ou serviços conexos, situados em território nacional ou que suportem serviços prestados no território nacional, essenciais para a continuidade do funcionamento das suas redes ou serviços, cuja indisponibilidade, degradação relevante, perda de integridade ou confidencialidade, perturbação ou destruição teria impacto significativo no funcionamento das suas redes e serviços.

OTT / *Over The Top* – Expressão usada para descrever os serviços disponibilizados através da Internet "aberta".

Plataforma de Resposta em Tempo Real - conjunto de ferramentas, sistemas e procedimentos que permite a detecção, análise, contenção e mitigação de incidentes de segurança de forma imediata ou com o mínimo de atraso possível, a fim de reduzir o impacto sobre os sistemas e dados da organização.

Artigo 2. São aditados os seguintes artigos:

ARTIGO 19

(Notificação de incidentes e informação ao público)

1. **Os incidentes de segurança com impacto grave devem ser notificados à Autoridade Reguladora e à ERIST no prazo máximo de vinte e quatro (24) horas a contar do conhecimento do incidente, sem prejuízo de comunicações ao CSIRT Nacional e a outras autoridades competentes, quando aplicável.**

2. **A notificação referida no número anterior deve incluir, pelo menos: descrição sumária do incidente, activos e serviços afectados, âmbito geográfico, medidas de mitigação em curso, impacto em clientes/utilizadores e prazos estimados de resolução.**

3. **No prazo de setenta e duas (72) horas após a resolução do incidente, incluindo a reposição do serviço quando aplicável, deve ser enviado à Autoridade Reguladora relatório final de incidente contendo, pelo menos, causas, medidas de remediação adoptadas e medidas de prevenção.**

4. **No prazo de dez (10) dias úteis após a resolução do incidente, incluindo a reposição do serviço quando aplicável, deve ser enviado à Autoridade Reguladora um relatório de incidente contendo as causas, as medidas de remediação e prevenção.**

5. **Consideram-se de impacto grave os incidentes que ultrapassem quaisquer dos seguintes limiares (salvo critérios específicos aprovados pela Autoridade Reguladora):**
   a) afectação de mais de cinco mil (5.000) utilizadores ou de mais de 1% da base do operador;
   b) indisponibilidade total por período superior a sessenta (60) minutos numa área;
   c) abrangência multi-provincial ou afectação de infra-estruturas críticas;
   d) violação de dados pessoais sensíveis.

6. **A comunicação ao público é obrigatória quando verificados os limiares definidos pela Autoridade Reguladora ou quando necessária para mitigar o impacto em utilizadores, devendo respeitar a legislação aplicável em matéria de proteção de dados e segurança.**

7. **A Autoridade Reguladora pode aprovar modelos e plataformas de reporte e formatos normalizados para as notificações previstas neste artigo.**

ARTIGO 20

(Detentores de infra-estruturas não operadores)

1. **As entidades detentoras ou gestoras de infra-estruturas aptas ao alojamento de redes de comunicações electrónicas que não sejam operadores de comunicações devem:**
   a) Designar um ponto de contacto de segurança;
   b) Implementar medidas proporcionais de segurança física e lógica;
   c) Notificar incidentes que afectem operadores alojados, nos termos do artigo 19.

2. **A Autoridade Reguladora pode emitir orientações técnicas específicas para estas entidades, incluindo procedimentos de coordenação com operadores, ERIST e CSIRT Nacional.**

ARTIGO 21

(Lista de activos e activos críticos)

1. **Os operadores devem remeter trimestralmente à Autoridade Reguladora a lista actualizada de activos críticos, com identificadores únicos, localização e função, em modelo e formato aprovados por aquela, podendo ser criada uma plataforma de Resposta em Tempo Real para o efeito.**

2. **As actualizações relevantes devem ser comunicadas no prazo de dez (10) dias úteis após a ocorrência.**

3. **A informação remetida ao abrigo deste artigo é de acesso restrito e tratada como confidencial, sem prejuízo das competências de auditoria e fiscalização da Autoridade Reguladora.**

Artigo 3. O presente Decreto entra em vigor na data da sua publicação.

Artigo 4. As obrigações decorrentes dos artigos 19 a 21 são implementadas no prazo de:

a) 90 dias para a designação de pontos de contacto, procedimentos de notificação e reporte;

b) 180 dias para a integração de alarmes em tempo real com a ERIST e envio periódico de activos críticos;

c) Um ano para a total conformidade com as obrigações do presente Decreto.