Quinta-feira, 1 de Agosto de 2019 I SÉRIE — Número 148

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

CONSELHO DE MINISTROS

Decreto n.º 66/2019

de 1 de Agosto

Tornando-se necessário estabelecer regras e procedimentos para garantir a segurança de redes e disponibilidade de serviços de telecomunicações, usando das competências atribuídas pela alínea *c*) do artigo 13 conjugado com o artigo 42, ambos da Lei n.º 4/2016 de 3 de Junho, Lei das Telecomunicações, o Conselho de Ministros determina:

Artigo 1. É aprovado o Regulamento de Segurança de Redes de Telecomunicações, em anexo, que é parte integrante do presente Decreto.

Art. 2. O presente Decreto entra em vigor 30 (trinta) dias após a sua publicação.

Aprovado pelo Conselho de Ministros, aos 9 de Abril de 2019.

Publique-se.

O Primeiro-Ministro, *Carlos Agostinho do Rosário*.

Regulamento de Segurança de Redes de Telecomunicações

CAPÍTULO I

Disposições Gerais

ARTIGO 1

(Definições)

O significado e definições dos termos, expressões e acrónimos utilizados no presente Regulamento constam do glossário em anexo, que dele faz parte integrante.

ARTIGO 2

(Objecto)

O presente Regulamento tem por objecto estabelecer procedimentos de execução de medidas técnicas a serem observadas em matéria de segurança e integridade da rede e infra-estruturas de telecomunicações.

ARTIGO 3

(Âmbito)

O presente Regulamento é aplicável aos operadores de redes e serviços públicos de telecomunicações na componente do funcionamento de segurança e integridade das redes e serviços.

ARTIGO 4

(Objectivos)

O presente Regulamento tem como objectivo a definição de normas e requisitos mínimos exigidos para a segurança das redes e serviços, de modo a garantir o seguinte:

a) Disponibilidade, integridade, confidencialidade e autenticidade;

b) Protecção de dados, transparência, qualidade das comunicações e resiliência da infra-estrutura de rede;

c) Controlo e monitoria da fraude nas comunicações, principalmente dada a adopção crescente da mobilidade no acesso às infra-estruturas da rede.

ARTIGO 5

(Atribuições da Autoridade Reguladora)

A Autoridade Reguladora, sem prejuízo de outras atribuições previstas na Lei, deve:

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

b) Liderar, promover e facilitar a identificação de fornecedores ou fabricantes de soluções mais eficazes contra a fraude de tráfego de telecomunicações.

CAPÍTULO II

Segurança nas Redes de Telecomunicações

ARTIGO 6

(Cooperação e partilha de informação)

1. Os operadores de redes e de serviços públicos de telecomunicações devem cooperar entre si no cumprimento das suas obrigações em matéria de segurança e integridade das redes e serviços, em especial, nas seguintes situações:

a) Riscos, ameaças ou vulnerabilidades que atingem os operadores;

b) Dependência ou interdependência entre as redes ou serviços, designadamente, o acesso e a interligação de redes, a co-localização de activos e a partilha de infra-estruturas ou de outros recursos;

c) Fornecimentos comuns de bens ou serviços por terceiros;

d) Necessidade de realizar acções conjuntas na celebração de acordos de assistência mútua, na troca de pontos de contacto permanentes ou da partilha de informação.

2. O operador de rede e de serviços públicos de telecomunicações em coordenação com a Autoridade Reguladora deve criar um serviço de denúncia de potenciais casos de fraude nos serviços de telecomunicações, onde o consumidor pode interagir com o operador.

3. O serviço indicado no número anterior deve permitir, que os potenciais números de SIM Box ou outros casos de fraude sejam bloqueados, após denúncia e devida investigação pela equipe do operador.

4. O operador de rede e de serviços públicos de telecomunicações e a Autoridade Reguladora devem designar um responsável pela segurança e um ponto de contacto permanente.

ARTIGO 7

(Protecção de dados e privacidade)

1. O operador de rede e de serviços públicos de telecomunicações deve assegurar a protecção e privacidade no controle e processamento de informações pessoais identificáveis do utilizador.

2. O operador de rede e de serviços públicos de telecomunicações deve adoptar mecanismos de protecção para impedir o acesso e uso de informações pessoais identificáveis pelo utilizador, garantindo que os conteúdos armazenados não possam ser usados por terceiros não autorizados.

3. O operador de rede e de serviços públicos de telecomunicações deve obter do consumidor o consentimento necessário para partilhar os seus dados pessoais identificáveis pelo utilizador.

4. O consentimento mencionado no número anterior também deve ser expresso e verificável por meio de prova.

5. Os dados pessoais dos residentes no território nacional devem ser armazenados dentro dos limites das fronteiras nacionais, regidos sob jurisdição de leis nacionais.

6. O operador de rede e de serviços públicos de telecomunicações que armazene dados pessoais dos consumidores na nuvem, fora do espaço territorial, deve garantir que os mesmos estejam sujeitos à jurisdição nacional, para além de sempre disponibilizar todo o tipo de informação quando solicitado pela Autoridade Reguladora ou outras Autoridades Competentes nos termos da Lei.

ARTIGO 8

(Obrigações do operador de telecomunicações)

1. O operador de rede e de serviços públicos de telecomunicações deve adoptar as medidas técnicas e organizacionais adequadas para garantir a integridade das respectivas redes, prevenção, gestão e redução dos riscos assegurando a continuidade da prestação do serviço público de telecomunicações dentro das suas plataformas.

2. O operador de rede e de serviços públicos de telecomunicações deve fortalecer a camada de protecção básica, tendo em vista o seguinte:

a) Construir e manter o inventário de dispositivos terminais e *softwares* de gestão da rede de telecomunicações autorizados;

b) Proteger as configurações em todos os sistemas de telecomunicações;

c) Executar a avaliação e correcção contínua de vulnerabilidades, tanto em redes a fio ou sem fio;

d) Desenvolver controlos de gestão de identidade e de acesso em torno de activos de telecomunicações;

e) Controlar e monitorar o nome do utilizador e a palavra-chave ou contas privilegiadas;

f) Manter, monitorar, analisar e auditar o registo de todas as actividades na infra-estrutura de rede;

g) Adoptar fortes medidas de segurança de redes sem fio;

h) Criar, dotar de meios e capacidade técnica a unidade de resposta e gestão de incidentes.

3. O operador de rede e de serviços públicos de telecomunicações deve melhorar as capacidades de detecção e resposta adoptando soluções de segurança que permitam obter visibilidade total e inteligência dos aplicativos, informações ou dados manuseados pelo pessoal de telecomunicações, de modo a detectar brechas de segurança.

4. O operador de rede e de serviços públicos de telecomunicações deve comunicar imediatamente aos seus consumidores, com conhecimento da Autoridade Reguladora, sobre as medidas adoptadas na sequência de ocorrência de qualquer tipo de fraude ou em relação a ameaças ou vulnerabilidades existentes.

5. O operador de rede e de serviços públicos de telecomunicações deve criar uma administração e gestão de identidade e acesso eficazes, designadamente:

a) Administração de acesso;

b) Serviços de autenticação e autorização;

c) Gestão de contas privilegiadas para pessoal do operador;

d) Serviços de acesso baseados em contexto para pessoal do operador;

e) Inteligência preditiva e análise do comportamento do utilizador para pessoal do operador.

6. O operador de rede de serviços públicos de telecomunicações deve desenvolver capacidades de recuperação de dados.

7. O operador de rede de serviços públicos de telecomunicações deve realizar testes de vulnerabilidades à segurança de redes e serviços de telecomunicações e enviar o respectivo relatório à Autoridade Reguladora, depois de acordados os seus termos.

8. O operador de rede e de serviços públicos de telecomunicações baseados em nuvem deve:

a) Ter planos de mitigação dos riscos que a adopção da Virtualização das Funções da Rede (NFV) pode trazer para segurança;

b) Monitorar os mecanismos de implantação, controlo e interligação dos elementos conectados numa Rede Definida por *Software* (SDN);

c) Assegurar a confidencialidade, integridade, disponibilidade e privacidade de todos os recursos e informações.

9. O operador de rede e de serviços públicos de telecomunicações que fornece ou está associado a provedores

de serviços de pagamento móvel deve, dentro da sua plataforma, solucionar as fraudes e os riscos relacionados com a verificação e provisionamento, vulnerabilidades de dispositivos e protecção de informações pessoais do cliente.

ARTIGO 9

(Requisitos de segurança)

1. O operador de rede e de serviços públicos de telecomunicações deve implantar as seguintes ferramentas:

a) Anti-Sonegação de Serviços Distribuídos;
b) *Firewall*;
c) IPS;
d) *Gateway* de Segurança no Sistema de Sinalização7;
e) Autenticação e Autorização de Utilizador;
f) Sistema de Monitoramento de Actividades de Banco de Dados;
g) Criptografia dos dados pessoais identificáveis pelo utilizador;
h) Ferramenta Avançada de Protecção de *Software* malicioso;
i) Outras ferramentas que se julgar necessárias.

2. O operador de rede e de serviços públicos de telecomunicações deve assegurar que as ferramentas comuniquem entre si e correlacionem o conjunto de informações usando uma gestão de eventos e informações de segurança.

3. O processo de monitoramento deve ser projectado para cobrir vários casos de uso de ataque em torno da infra-estrutura de telecomunicações.

4. Para efeitos do número anterior, o operador de rede e de serviços públicos de telecomunicações deve ser submetido a diferentes auditorias, internas e externas, com finalidade de aferir a eficácia operacional de vários controlos de segurança que emanam desses vários padrões.

5. O operador de rede e de serviços públicos de telecomunicações deve assegurar a resiliência e disponibilidade dos sistemas, por meio das seguintes medidas:

a) Redundâncias na infra-estrutura da espinha dorsal, através de alocação do tráfego em rotas físicas ou lógicas distintas;
b) Redundâncias nos sistemas de energia e ar-condicionado, quando aplicável;
c) Sistemas de controlo de acesso e de protecção contra incêndio.

6. O operador de rede e de serviços públicos de telecomunicações deve usar recursos de telemetria com vista ao envio de um sinal de alarme para o Centro de Operações de Rede, quando se detectar o seguinte:

a) Falha da unidade de controlo;
b) Remoção de bateria de redundância ou ventilador;
c) Acesso não autorizado ao *site* ou sala de equipamentos.

7. As mensagens enviadas do Centro de Operações de Rede para os equipamentos remotos devem ser protegidas contra compromissos ou falsificações maliciosas por utilizadores não autorizados.

8. O operador de rede e de serviços públicos de telecomunicações deve implementar a Gestão Segura de Rede de modo a proteger os equipamentos contra a má configuração acidental ou não intencional da rede.

ARTIGO 10

(Serviço de pagamento móvel)

1. No serviço de pagamento móvel deve ser assegurada a separação dos servidores de SMS ordinários dos servidores das SMS de transações financeiras.

2. Não sendo possível a separação prevista no número anterior deve ser elevado o nível de mecanismos de segurança.

ARTIGO 11

(Procedimento de controlo)

O operador de rede e de serviços públicos de telecomunicações, deve observar os seguintes procedimentos de controlo:

a) Realizar avaliações periódicas e completas dos riscos de segurança da infra-estrutura de telecomunicações para cobrir todas as camadas de comunicação, tais como rede aplicativos, dados, identidade, acesso e processos em várias tecnologias;
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;
c) Denunciar ou reportar para a Autoridade Reguladora os incidentes de segurança ou violações das redes e sistemas comerciais que processam dados identificáveis pelo utilizador;
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.

ARTIGO 12

(Procedimentos de gestão de alterações da rede)

1. O operador de rede e de serviços públicos de telecomunicações deve estabelecer mecanismos com o fim de minimizar a probabilidade de ocorrência de incidente de segurança que possa resultar dessas alterações.

2. No caso de alterações físicas ou lógicas aos activos classificados como críticos, deve-se acrescentar os seguintes procedimentos:

a) Realização de testes de integração e de sistema antes da introdução da alteração;
b) Elaboração do plano de restauro dos activos, adequado ao tipo da alteração a introduzir.

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.
b) Rever os Sistemas de Controlo de Acessos com uma periodicidade mínima anual e sempre que necessário, em função das Análises dos Riscos realizadas, bem como efectuar testes com uma periodicidade mínima semestral, com vista à protecção contra acessos não autorizados.

c) Assegurar a documentação e o registo da operação dos Sistemas de Controlo de Acessos, que inclua:

i) As alterações introduzidas;
ii) Os incidentes de segurança ocorridos;
iii) Os testes realizados;
iv) Os alarmes gerados.

ARTIGO 14

(Sistemas de monitorização e controlo da segurança)

1. Na adopção do sistema de Monitorização e Controlo da Segurança o operador de rede e de serviços públicos de telecomunicações deve estabelecer e manter condições de funcionamento, da segurança e integridade dos activos constantes do Inventário de activos e do tráfego, que operem continuamente de modo a permitir o seguinte:

a) A detecção de ameaças e de incidentes de segurança;
b) A geração dos alarmes adequados no caso da sua ocorrência;
c) A activação de medidas de segurança.

2. O sistema de monitorização e controlo deve ser adequado à prevenção, à gestão e à redução dos riscos para o funcionamento e para a segurança e integridade das redes e serviços.

3. O sistema de monitorização e controlo deve ser revisto com uma periodicidade mínima anual ou sempre que necessário, principalmente em função das Análises dos Riscos realizados, bem como realizar testes com periodicidade mínima semestral.

4. O sistema de monitorização e controlo deve possuir documentação e registo de operação que inclua o seguinte:

a) As ameaças detectadas;
b) Os incidentes de segurança ocorridos;
c) Os alarmes gerados;
d) As medidas activadas;
e) Os testes realizados;
f) As alterações introduzidas.

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) A política de segurança;
b) A informação sobre a abordagem e a metodologia de segurança e de gestão dos riscos adoptadas;
c) A descrição do sistema de gestão de segurança;
d) A descrição das medidas de redundância, de robustez e resiliência da rede;
e) A descrição do Sistema para a Monitorização do Tráfego de Acesso à *Internet* quando aplicável;
f) A descrição dos Sistemas de Controlo de Acessos;
g) A descrição dos Sistemas de Monitorização e Controlo;
h) 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. O Plano de Segurança consiste na elaboração de todas medidas técnicas e organizacionais adoptadas pelos operadores de redes e de serviços públicos de telecomunicações.

2. O Plano de Segurança deve ter como objectivos gerais, os seguintes:

a) Garantir a segurança e a integridade, físicas e lógicas, das redes e de serviços;
b) Recuperar rapidamente o funcionamento das redes e serviços em caso de ocorrência de incidente de segurança;
c) Melhorar o nível de segurança e integridade das redes e de serviços;
d) Assegurar a coordenação das acções entre os operadores de redes e de serviços públicos de telecomunicações e as demais entidades envolvidas, incluindo a Autoridade Reguladora.

3. O Plano de Segurança deve também incluir em especial, o seguinte:

a) Plano de continuidade ou de restauro específicos para os activos constantes do inventário de activos críticos;
b) As medidas necessárias para a salvaguarda de reserva de capacidade para comunicações de emergência de interesse público;
c) As medidas necessárias em matéria de congestionamento de redes em situações de emergência, incluindo os procedimentos a cumprir pelo operador de rede e de serviços públicos de telecomunicações.

ARTIGO 17

(Responsável pela segurança)

O responsável pela segurança é a pessoa encarregue de, entre os demais deveres previstos no presente Regulamento, responder pelo seguinte:

a) Pela gestão da política de segurança;
b) Pela gestão do sistema de segurança;
c) Pela promoção do cumprimento das obrigações do operador de rede e de serviços públicos de telecomunicações, em matéria de segurança e integridade das redes e serviços, ao abrigo do disposto na Lei e no presente Regulamento.

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.

CAPÍTULO III

Regime Sancionatório

ARTIGO 19

(Sanções e multas)

A falta de cumprimento das obrigações resultantes da aplicação do presente Regulamento constitui infracção e está sujeito às seguintes multas:

a) 100.000,00 MT por falta de protecção dos dados e privacidade de cada consumidor, conforme mencionado nos n.ºs 1, 2 e 3 do artigo 7;

b) 10.000.000,00 MT por falta de adopção de medidas adequadas à prevenção e gestão de risco mencionadas no n.º 1 do artigo 8;

c) 500.000.00 MT por falta de fortalecimento da camada de protecção básica exigida, em qualquer das alíneas do n.º 2 do artigo 8;

d) 500.000.00 MT por falta de realização de teste de vulnerabilidade à segurança de redes e não envio dos mesmos a Autoridade Reguladora, nos termos do n.º 6 do artigo 8;

e) 5.000.000,00 MT por falta de uma das obrigações constantes em qualquer das alíneas referidas no n.º 8 do artigo 8;

f) 5.000.000,00 MT por falta de solução de fraudes e os riscos relacionados com os serviços de pagamento móvel, conforme o n.º 9 do artigo 8.

ARTIGO 20

(Aplicação da multa)

1. À Autoridade Reguladora compete aplicar e cobrar as multas previstas no presente Regulamento mediante notificação ao operador de rede e de serviços públicos de telecomunicações, infractor, para pagamento da mesma.

2. A notificação deve conter a matéria acusatória e todos os elementos de prova produzidos, incluindo a cópia do auto de notícia.

3. O operador de rede e de serviços públicos de telecomunicações, infractor, tem 10 (dez) dias úteis contados a partir da data de notificação para, querendo, exercer o seu direito de defesa.

4. A Autoridade Reguladora deve tomar a decisão no prazo de 10 (dez) dias úteis contados a partir da data da recepção da defesa do infractor.

5. Quando o infractor não for encontrado ou se recusar a receber a notificação, a mesma é feita através de anúncios em quatro números seguidos de um dos jornais de maior circulação na localidade da última residência do notificando ou de maior circulação nacional.

6. O exercício do direito de defesa interrompe a contagem do prazo para o pagamento da multa.

7. O infractor tem o prazo de 20 (vinte) dias úteis a contar da data da recepção da notificação ou da decisão para proceder o pagamento da multa.

8. O operador de rede e de serviços públicos de telecomunicações, infractor, tem um prazo de 90 (noventa) dias a contar da data da recepção da notificação para sanar as causas que ditaram a aplicação da multa.

9. A Autoridade Reguladora acciona os mecanismos de execução fiscal, caso o infractor não efectue o pagamento voluntário da multa aplicada.

ARTIGO 21

(Destino das multas)

1. Compete aos Ministros que superentendem as Áreas das Comunicações e das Finanças definir a percentagem do destino dos valores das multas.

2. O valor das multas deve ser canalizado a Conta Única do Tesouro (CUT) e consignado à Autoridade Reguladora no prazo de 5 (cinco) dias, após a sua cobrança.

ARTIGO 22

(Reincidência)

1. Em caso de reincidência o valor das multas previstas no presente Regulamento será elevado ao dobro.

2. Para efeito do presente Regulamento, a reincidência consiste no cometimento da mesma infracção antes de ter decorrido um ano, contados da data da fixação da sanção anterior.

ARTIGO 23

(Recurso)

1. O infractor pode, no prazo de 5 (cinco) dias úteis após a recepção da decisão apresentar recurso hierárquico ao Conselho de Administração da Autoridade Reguladora.

2. O Conselho de Administração da Autoridade Reguladora decide sobre o recurso no prazo máximo de 30 (trinta) dias, a contar da data da sua recepção, sem prejuízo de eventuais prorrogações.

3. Das decisões tomadas no âmbito do presente Regulamento cabe recurso nos termos da lei.

ARTIGO 24

(Auto de notícia)

1. O auto de notícia lavrado no cumprimento das disposições do presente Regulamento faz prova sobre os factos presenciados pelos autuantes, até prova em contrário.

2. O disposto no número anterior aplica-se também aos elementos de prova obtidos através de aparelhos ou instrumentos aprovados nos termos legais.

3. Do auto de notícia deve constar o endereço do autuado, sendo este advertido de que o endereço fornecido vale para efeitos de notificação.

ARTIGO 25

(Fiscalização)

1. A Autoridade Reguladora deve periodicamente ou sempre que justificado auditar ou fiscalizar bem como solicitar a demonstração da conformidade com os aspectos de segurança mencionados no presente Regulamento.

2. A auditoria ou fiscalização mencionada no número anterior pode ser feita pela Autoridade Reguladora ou por mandatários devidamente credenciados.

CAPÍTULO IV

Disposições Transitórias

ARTIGO 26

(Prazos)

1. Os operadores de redes e de serviços públicos de telecomunicações em actividade à data da entrada em vigor do presente Regulamento devem:

a) No prazo de 30 (trinta) dias úteis a contar da data de entrada em vigor do presente Regulamento, estabelecer a função de Responsável pela Segurança, comunicando à Autoridade Reguladora, dentro do mesmo prazo;

b) No prazo de 45 (quarenta e cinco) dias úteis a contar da data de entrada em vigor do presente Regulamento, estabelecer a função de Ponto de Contacto Permanente, comunicando à Autoridade Reguladora, dentro do mesmo prazo.

2. No prazo de 180 (cento e oitenta) dias a contar da data de entrada em vigor do presente Regulamento, iniciar a implementação das seguintes acções:

a) Adoptar os procedimentos de gestão de alterações;

b) Adoptar um sistema de controlo de acessos;

c) Adoptar um sistema de monitorização e controlo;

d) Assegurar o acesso aos serviços à Equipa de Resposta a Incidentes de Segurança;

e) No prazo de um ano, a contar da data em que se acorda o formato do relatório elaborar um relatório anual de segurança, e submeter à Autoridade Reguladora;

f) No prazo de 36 (trinta e seis) meses a contar da data de entrada em vigor do presente Regulamento, adoptar as medidas de redundância e resiliência da rede e infra-estruturas de telecomunicações.

Glossário

A

1. **Acesso não autorizado** – Passagem ou circulação não autorizada à rede para uso dos serviços.

2. **Análise preditiva** – Categoria de estudo de dados focada em fazer previsões sobre dados passados e actuais para prever com segurança tendências e comportamentos futuros.

3. **Ataque de negação de serviço distribuído** – Acto malicioso de interromper o tráfego normal de um servidor, serviço ou rede, por meio da sobrecarga do alvo ou de sua infra-estrutura, com uma inundação de tráfego de *Internet*.

4. **Autoridade Reguladora** - Instituição pública que desempenha as funções de regulação, supervisão, fiscalização e representação do sector de telecomunicações, que é a Autoridade Reguladora das Comunicações - INCM.

C

1. **Camada de protecção básica** – Porção ou revestimento que controla a execução do acesso ou conexão com a rede do operador pelos próprios colaboradores, onde toda troca de informações pressupõe uma conexão ainda que temporária entre duas máquinas por onde essa troca vai ocorrer.

2. **Computação em Nuvem** – Modelo no qual o processamento, o armazenamento e os *softwares* são oferecidos por um provedor de serviços permitindo o acesso a serviços *on-line* sem a necessidade de instalar programas localmente, sendo acessados pelos utilizadores remotamente, via *Internet*.

3. **Conteúdo digital** - Aquilo que está contido ou encerrado em formato digital ou código binário, que contém informações e que podem ser enviadas através de ondas de rádio, *stream* via *Internet* ou arquivo de computador a serem consumidas de modo gratuito ou pago por pessoas físicas ou jurídicas.

4. **Criptografia** - Mecanismo de segurança e privacidade que torna determinada comunicação em forma de textos, imagens, vídeos, ou outros, ininteligível para quem não tem acesso aos códigos de interpretação da mensagem.

E

1. **ERB falsa** - Equipamento que permite a conexão entre os telefones celulares e a companhia telefónica por via da Central de Comutação e Controle usado ilegalmente por pessoas não autorizadas para fins fraudulento.

2. **Espionagem** – Acto de um invasor poder espiar ou interceptar dados importantes ou ligações telefónicas confidenciais no tráfego da interface aérea não fortemente criptografado.

F

1. *Firewall* – Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

2. **Fraude de tráfego de telecomunicações** – Acto de má fé praticado com objectivo de enganar ou prejudicar o consumidor e o operador de telecomunicações nas operações que ocorram na rede de telecomunicações.

G

1. ***Gateway* de Segurança no Sistema de Sinalização 7** – É a componente de rede usado para enviar mensagens de sinalização entre nós de sinalização de canal comum (CCS), que se comunicam com a ajuda de diferentes transportes e protocolos.

2. **Gestão de identidade e acessos** - Processo pelo qual se organiza e administra as relações entre pessoas e activos de rede ou infra-estrutura de telecomunicações durante todo o ciclo de relacionamento entre o consumidor e operador.

3. **Gestão Segura de Rede** – Solução que permite obter um alto nível de visibilidade do comportamento da rede, automatizar a configuração de dispositivos, aplicar directivas globais, visualizar o tráfego de *firewall*, gerar relatórios e fornecer uma única interface de gestão para sistemas físicos e virtuais.

4. **GSM *Gateways*** - Equipamentos que permitem o roteamento directo entre redes IP, digitais e analógicas para as redes GSM de telefonia celular.

I

1. **Incidente de segurança** - Qualquer evento adverso, como confidencialidade, integridade, disponibilidade, autenticidade ou outros, confirmando ou sob suspeita, relacionado à segurança que pode levar a perda de um ou mais princípios básicos de Segurança da rede.

2. **Infra-estrutura de telecomunicações** - Conjunto de equipamentos, Sites físicos, Contentores de equipamento, estruturas e instalações usadas para viabilizar o fornecimento de serviços de telecomunicações.

3. **Invasor-no-meio** - Atacante que pode estar entre um telefone celular e um ponto de acesso da rede para interceptar mensagens, por meio de um *hotspot* malicioso, para prejudicar o consumidor.

4. **IPS** - "Sistema de Prevenção contra Intrusos" Sistema que permite o armazenamento de *logs* e técnicas avançadas de alertas e respostas, dedicado exclusivamente a tornar infra-estrutura cada vez mais segura, sem perder o grau de disponibilidade que uma rede.

N

Negação de serviço – Envio excessivo de dados na rede, mais do que ela pode suportar, deixando os utilizadores sem os recursos de rede disponíveis.

O

1. **Obstrução do meio** - Técnica usada pelos invasores cujo objetivo é destruir ou degradar o sinal da interface aérea, desabilitando o acesso dos utilizadores legítimos dessa rede deixando-os expostos a "outras" redes.

2. **Operador de telecomunicações** – Qualquer sociedade comercial, licenciada pela Autoridade Reguladora que se dedique à exploração de uma rede pública de telecomunicações podendo também prestar serviços de telecomunicações ao publico em geral.

3. **Operador de redes** - Qualquer sociedade comercial, que se dedique à exploração ou gestão de uma rede pública de telecomunicações, podendo também prestar serviços de telecomunicações ao público em geral.

P

1. **Pagamento Móvel** - Conjunto de soluções que permitem realizar transações financeiras como os meios de pagamento, através do uso de dispositivos móveis.

2. **Protocolo *IP/MPLS*** - Multiprotocolo de roteamento baseado em pacotes rotulados, para tornar mais eficiente o encaminhamento e comutação de pacotes na rede.

R

1. **Rede baseada em nuvem** – Sistama de elementos centralizados em substituição de uma infra-estrutura física tradicional de rede que normalmente é exigido como componente individual de servidor, armazenamento, computação ou infra-estrutura adquiridos e montados para suportar um serviço.

2. **Rede de telecomunicações** – Sistema de telecomunicações interligado e integrado constituído por vários meios de transmissão e comutação, utilizados para fornecer serviços de telecomunicações.

3. **Rede de Telecomunicações Baseadas em Nuvem** – Sistema que consiste em *hardware*, como componentes de rede, armazenamento e de *software*, que permitem a virtualização, ferramentas de gestão e segurança que hospedam "máquinas virtuais," que podem ser geridas por meio de interfaces baseadas em navegadores.

4. **Rede Definida por *Software* (SDN)** – Sistema que usa *software*. em vez de dispositivos especializados, para provisionar e gerir serviços de redes e aplicativos, permitindo fornecimento e mobilidade de aplicativos programáveis, expansíveis e sob demanda.

S

1. **Segurança** – Percepção de se estar protegido de riscos, perigos ou perdas.

2. **Segurança de Redes** – Conjunto de recursos que consiste na provisão e adopção de políticas para prevenir e monitorar riscos, perigos ou perdas, decorrentes de acessos não áutorizados, uso incorrecto, modificação ou negação da rede e dos seus recursos associados.

3. **Segurança física** – Forma de proteger fisicamente equipamentos e informações contra utilizadores que não possuem autorização para acessá-los.

4. **Segurança lógica** – Conjunto de recursos executados para proteger o sistema, dados e programas contra tentativas de acessos de pessoas ou por programas desconhecidos.

5. **Sequestro de sessão** – Acto malicioso de retenção de uma sessão já estabelecida actuando como um legítimo utilizador de uma determinada estação de base.

6. **Serviço de pagamento móvel** – Actividade de pagamento móvel que consiste em prover mecanismos de remuneração através da plataforma de telecomunicações.

7. ***SIM BOX*** - Dispositivo usado como parte de uma instalação de *gateway* ou *VoIP*, com vários cartões *SIM* instalados e armazenados separadamente.

8. **Sistema de controlo de acessos** – Conjunto de recursos cujo objectivo é de controlar quem pode estar num dado momento, num determinado local.

9. **Sistemas de suporte ao negócio** – Conjunto de recursos que os operadores de serviços usam para executar suas operações de negócios.

10. **Sistemas de Suporte à Operação** - Conjunto de recursos usada para executar funções de gestão, inventário, engenharia, planeamento e função de reparação dos operadores de serviços de telecomunicações e suas redes.

11. ***Software* malicioso** – Código ou programa de computador desenvolvido com objectivo de informar se em sistema de rede de forma ilícita com intuito de causar danos.

12. **Subsistema Multimédia IP** – Elementos de rede que constituem a estrutura responsável pela distribuição de multimédia (voz, vídeo, dados e outro), independentemente do dispositivo terminal ou do meio de acesso , através do protocolo IP.

T

Teste de penetração – Método que avalia a segurança de um sistema,.rede ou de infra-estrutura, simulando um ataque de uma fonte maliciosa.

V

Vulnerabilidades- Fraquezas que permitem ataques do tipo *Man-in-the-Middle* no uso de *Rogue* BTS (ERB falsa), o qual obstrui o sinal da operadora para que o terminal móvel busque uma outra rede, recorrendo-se então a Estação Rádio Base (ERB) falsa.

Resolução n.º 39/2019

de 1 de Agosto

Havendo necessidade de se desativar o Alerta Vermelho na Região Centro do País, ativado através da Resolução n.º 12/2019, de 13 de Março, na iminência do Ciclone Idai, ao abrigo do n.º 2 do artigo 16 da Lei n.º 15/2014, de 20 de Julho, Lei que estabelece o Regime Jurídico da Gestão de Calamidades, e sob proposta do Conselho Coordenador de Gestão de Calamidades, o Conselho de Ministros determina:

Artigo 1. A desativação do Alerta Vermelho na Região Centro do País, nomeadamente, nas Províncias de Tete, Zambézia, Sofala e Manica.

Art. 2. A presente Resolução entra imediatamente em vigor.

Aprovada pelo Conselho de Ministros, aos 7 de Maio de 2019. — O Primeiro-Ministro, *Carlos Agostinho do Rosário.*