Região Administrativa Especial de Macau

Lei da Cibersegurança

Documento de consulta

Período de Consulta Pública: 11 de Dezembro de 2017 a 24 de Janeiro de 2018

Governo da Região Administrativa Especial de Macau

2017

Índice

Introdução……3

1. Criação do sistema de protecção da cibersegurança…….……....7

2. Definições relativas às infraestruturas críticas e à cibersegurança…….....….9

3. Âmbito de aplicação do sistema de protecção da cibersegurança……..……11

3.1. Operadores públicos das infraestruturas críticas – órgãos, serviços e entidades públicos.....11

3.2. Operadores privados das infraestruturas críticas…….…….…11

4. Entidades supervisoras do Governo…...…….……13

4.1. Comissão Permanente para a Cibersegurança….……...……...…14

4.2. Centro de Alerta e Resposta a Incidentes de Cibersegurança……...14

4.3. Entidades supervisoras do Governo nos diversos domínios.…….……...……15

5. Deveres legais……..…17

5.1. Deveres de carácter orgânico……17

5.2. Deveres de carácter procedimental, preventivo e reactivo ……...…...18

5.3. Deveres de auto-avaliação e relato…….…….....……..19

5.4. Dever de colaboração..……...…….. 19

5.5. Deveres específicos dos operadores da rede pública..……..19

5.6. Deveres dos operadores públicos das infra-estruturas críticas…….....…20

6. Incumprimento dos deveres e respectivas sanções administrativas e responsabilidades disciplinares……...….21

7. Ponderações especiais sobre a data da entrada em vigor……...……23

8. Regulamentação..……..…..……. 23

Tabela para sugestões e opiniões acerca da proposta da "Lei de Cibersegurança"…….……24

Introdução

A tecnologia informática é inseparável das actividades dos diversos sectores e profissões, bem como da vida quotidiana dos cidadãos da RAEM, sendo os equipamentos informáticos, tais como computadores e telemóveis, e a internet ferramentas indispensáveis do dia-a-dia.

Por outro lado, as inovações tecnológicas, nomeadamente a "internet móvel", "internet plus", "serviços de núvem", "internet das coisas" e "inteligência artificial", têm registado também uma rápida e ampla aplicação, sendo a rede considerada como um novo canal de transmissão de informação, um novo espaço de produção e de vida, um novo motor de desenvolvimento da economia, um novo suporte de prosperidade cultural, uma nova plataforma de governação da sociedade, uma nova ponte de intercâmbio e de cooperação, assim como um novo domínio da soberania estatal.

Contudo, estamos perante um cenário internacional marcado pela complexidade e mudanças constantes, o terrorismo tem-se alargado a uma escala global e os diversos tipos de crime têm superado os limites territoriais, sendo as lacunas de alto risco nos sistemas informáticos aproveitadas para a actuação transfronteiriça e globalizada. Por isso, a diversificação dos ataques e das invasões na rede e a ligação da cibersegurança com a segurança nacional e a segurança pessoal passaram a ser o foco de atenção dos governos dos diversos países e regiões desenvolvidos, os quais têm avançado com a regulação da cibersegurança, através de leis próprias.

A RAEM já não pode manter-se à parte desta situação, sendo imprescindível sintonizar-se com a tendência global e progredir no trabalho legislativo, de modo a promover o bom funcionamento dos sistemas da rede e garantir a integridade e a protecção suficiente dos dados da rede, isto tudo, para criar um sistema de gestão preventivo sólido para as infra-estruturas críticas da sociedade que permite uma melhor articulação com a estratégia nacional de desenvolvimento, "Uma Faixa, uma Rota" e os objectivos do Plano Quinquenal de Desenvolvimento da RAEM (2016-2020), nomeadamente a construção de uma cidade inteligente e a conjugação das indústrias com a internet.

Por conseguinte, em 2015, segundo a indicação dada por Sua Excelência o Senhor Chefe do Executivo, foi criado um grupo de trabalho interdepartamental de Cibersegurança, cabendo ao Secretário para a Segurança a coordenação dos serviços competentes no desenvolvimento do trabalho legislativo e na criação de unidades de serviços de cibersegurança da RAEM. Em 2016, logo após

a definição do plano de trabalho e do quadro geral da cibersegurança, o grupo iniciou o trabalho de elaboração do projecto da lei-quadro da cibersegurança, sendo a Lei de Cibersegurança concebida com base nos seguintes três princípios:

1. Garantia da segurança da população e respeito pela privacidade das pessoas;

2. Proporcionalidade legislativa (nomeadamente nos âmbitos da aplicação da lei e das medidas técnicas);

3. Simplicidade e eficácia do enquadramento institucional

O estabelecimento do regime jurídico de cibersegurança depende da participação activa dos diversos sectores da sociedade, designadamente dos operadores das infra-estruturas críticas que são estreitamente ligados à vida quotidiana da população em geral. Assim, o Governo da RAEM espera dar a conhecer ao público, da forma mais transparente possível, os objectivos e a intenção legislativa original, com vista a auscultar amplamente as opiniões dos diversos sectores, optimizando assim a tarefa de criação deste regime

Face ao exposto, convidamos sinceramente as individualidades dos diversos sectores (incluindo cidadãos, empresas e instituições) a apresentarem, por escrito, as suas sugestões ou opiniões sobre o conteúdo do presente documento de consulta através de quaisquer dos meios abaixo indicados:

1. Período de consulta:

   11 de Dezembro de 2017 a 24 de Janeiro de 2018.

2. Meios de apresentação das sugestões ou opiniões:

   (1) Por carta: através de correio ou entrega directa ao **Gabinete do Secretário para a Segurança, sito na Calçada dos Quartéis da RAEM**, ou à **Direcção dos Serviços da Administração e Função Pública, sita na Rua do Campo, nº 162, Edifício "Administração Pública", 27º andar, Macau**.

   (2) Por via electrónica: através do acesso à página electrónica específica no Portal do Governo da Região Administrativa Especial de Macau (http://portal.gov.mo/pt) ou no website do Gabinete do Secretário para a Segurança (www.gss.gov.mo/pt/ciberseg).

3. Na capa de sugestões ou opiniões: Por favor especifique na capa ou no cabeçalho da folha de sugestões ou opiniões o seguinte: "**Sugestões e Opiniões sobre a Lei de Cibersegurança**".

4. Conteúdo das sugestões e opiniões e a respectiva declaração de confidencialidade: Relativamente à apresentação de sugestões e opiniões, agradecemos que tenha como referência a "**Tabela de sugestões e opiniões acerca da proposta da "Lei de Cibersegurança"** anexa ao presente documento de consulta. Caso pretenda manter a confidencialidade das suas opiniões e sugestões, queira indicá-lo expressamente na coluna correspondente.

   O presente documento de consulta encontra-se disponível no website do Gabinete do Secretário para a Segurança: www.gss.gov.mo/pt/ciberseg.

1. Criação do sistema de protecção da cibersegurança.

Relativamente ao regime jurídico em matéria de informática e da rede, actualmente, existe somente a Lei n.º 11/2009 (Lei de combate à criminalidade informática) que regula os crimes cibernéticos e as respectivas penas, mas não há nenhuma lei nem regulamento que se destine exclusivamente à matéria de gestão preventiva com natureza administrativa no âmbito da cibersegurança.

A cibersegurança está estreitamente ligada à segurança nacional e à vida quotidiana dos cidadãos, a sua prevenção é a melhor solução; contudo, é impossível que esta tarefa seja só da responsabilidade do Governo. O trabalho da prevenção deve contar com a participação activa dos vários sectores sociais. A eficácia na defesa da cibersegurança só pode ser conseguida quando o Governo, os sectores da sociedade e toda a população estão unidos e cooperam mutuamente.

Nesse sentido, tendo tomado como referência o regime jurídico relacionado com esta matéria da China continental e de outros países ou regiões, o Governo da RAEM considera que é imprescindível preencher o vazio legal existente. Pretende-se, em cumprimento do princípio de "garantia da segurança da população e respeito para a privacidade das pessoas", criar um sistema de protecção no âmbito de cibersegurança para Macau, e que se caracteriza por um sistema de gestão preventivo com natureza administrativa, no qual se estipulam explicitamente os deveres e responsabilidades de todas as partes nesta matéria.

Deste modo, a "Lei de Cibersegurança" que o Governo pretende estabelecer é uma lei com objectivo de "protecção", "prevenção" e "gestão" e, através da supervisão do cumprimento dos deveres relativos à cibersegurança pelos operadores das infra-estruturas críticas e da monitorização da dimensão do fluxo dos dados informáticos e das características dos datagramas, etc., entre as redes das infra-estruturas críticas e a internet, conhecer a situação de cibersegurança, com vista a:

- prevenir, detectar e combater as invasões e os ataques cibernéticos, garantir a segurança das redes das infra-estruturas críticas, salvaguardar a segurança pública, o interesse público e a ordem pública da RAEM;

- reagir aos incidentes de cibersegurança, promover os deveres e medidas relativos à cibersegurança, optimizar o regime de gestão preventivo da cibersegurança;

- emitir alertas sobre incidentes, evitar ou reduzir a ocorrência de incidentes nas infra-estruturas críticas, bem como desenvolver acções de divulgação e sensibilização específicas, reforçar a consciência nesta área nos operadores das infra-estruturas críticas.

Entretanto, os ilícitos penais ligados à rede, à informática e aos computadores

continuarão a ser regulados pela Lei de combate à criminalidade informática.

Dado que os mecanismos e medidas de protecção concretas da cibersegurança irão ser actualizadas e ajustadas em qualquer altura conforme as circunstâncias, dando ênfase ao profissionalismo e tecnicidade, sugerimos que, conforme o princípio de proporcionalidade legislativa, a proposta da "Lei de Cibersegurança" não regule directamente as medidas concretas a nível da defesa da cibersegurança, nomeadamente, os critérios de escolha de *firewall,* sistema de criptografia, autenticação electrónica, sistema de detecção de invasão de vírus, entre outros.

As medidas referidas irão ser reguladas pelas instruções e circulares emitidas pelas entidades supervisoras, tendo em conta as orientações gerais definidas pelo Governo.

2. Definições relativas às infra-estruturas críticas e à cibersegurança.

O funcionamento normal da sociedade e o dia-a-dia dos próprios cidadãos estão estreitamente ligados aos serviços prestados pelas infra-estruturas, por exemplo, o abastecimento de água e fornecimento de energia (electricidade e gás natural); transportes terrestres, marítimos e aéreos; teledifusão e radiodifusão; rede pública inclusive serviços da internet; serviços bancário, financeiro e seguros; serviços médicos; serviços públicos (serviços fornecidos pela administração pública), entre outros. Em casos de ataques às redes informáticas e sistema de infra-estruturas críticas, cujo dano, revelação de dados ou perda da função possa causar grande impacto social ou até paralisar o funcionamento do Governo e da sociedade, provocando directamente riscos à segurança pública e à ordem pública, bem como o bem-estar dos cidadãos, isso irá trazer inevitavelmente graves e incalculáveis consequências para a sociedade.

Considerando que a China continental, países europeus e americanos desenvolvidos, Rússia, Singapura, RAEHK, região de Taiwan etc., têm garantido sucessivamente, uma protecção a nível elevado das "infra-estruturas estratégicas" supracitadas mediante leis e outras medidas complementares, sugerimos que, ao legislar, os operadores das infra-estruturas acima referidas sejam definidos como "operadores das infra-estruturas críticas", e são definidos os seus deveres de cibersegurança, aperfeiçoando assim o sistema preventivo de gestão no âmbito da cibersegurança.

Para esclarecer as expressões relacionadas com a cibersegurança, sugerimos que sejam adoptadas as seguintes definições:

"Infra-estruturas críticas": patrimónios, sistemas e redes que se consideram relevantes para o interesse da sociedade e para o seu funcionamento normal, cujo dano, revelação de dados ou a perda da função poderá causar prejuízos graves para a segurança pública, o interesse público e a ordem pública, independentemente da natureza pública ou privada dos seus operadores.

"Operadores das infra-estruturas críticas": entidades públicas ou privadas que operam as infra-estruturas críticas ou que prestam serviços ligados às mesmas.

"Rede": sistemas interligados, compostos por computadores ou por outros terminais informáticos e respectivos equipamentos, que efectuam, segundo certas regras e procedimentos, à recolha, armazenamento, troca, transmissão e tratamento de dados.

"Dados da rede" são dados digitais recolhidos, armazenados, transmitidos, tratados e produzidos através da rede.

"Cibersegurança", a actividade permanente e plurisectorial desenvolvida pela

RAEM, no sentido de garantir a segurança das redes informáticas essenciais, utilizadas pelos operadores das infra-estruturas críticas, de modo a preservar a integridade, confidencialidade e disponibilidade dos dados que circulam nas mesmas e prevenir que as redes sejam atingidas por incidentes ou actos não autorizados, nomeadamente a aquisição, invasão, utilização, controle, interferência, revelação, danificação, alteração e destruição.

"Incidentes de cibersegurança": são aqueles que possam causar ou tenham causado dano ou prejuízo ao funcionamento da rede ou à confidencialidade, integridade e disponibilidade dos dados da rede em operação.

3. Âmbito de aplicação do sistema de protecção da cibersegurança.

De acordo com as definições acima referidas, por "operadores das infra-estruturas críticas" entendem-se dois sectores, público e privado, os quais devem assumir um certo grau de responsabilidade pela cibersegurança das "infra-estruturas críticas" importantes, sem margem para qualquer falha.

3.1. Operadores públicos das infra-estruturas críticas – órgãos, serviços e entidades públicos.

A expressão sugerida integra todos os órgãos, serviços e entidades públicos, compreendendo:

(1) O Gabinete do Chefe do Executivo, os gabinetes dos titulares dos principais cargos do Governo e os respectivos serviços de apoio administrativo, os serviços de apoio à Assembleia Legislativa, o Gabinete do Presidente do Tribunal de Última Instância, o Gabinete do Procurador, o Gabinete do Comissariado Contra a Corrupção e o Gabinete do Comissariado da Auditoria;

(2) Institutos públicos e fundos autónomos, qualquer que seja a modalidade que estes revistam;

(3) Demais serviços e organismos públicos que, embora desprovidos de personalidade jurídica, possuam autonomia patrimonial e financeira.

No entanto, estão excluídos do âmbito de aplicação do presente regime jurídico os órgãos, serviços e entidades da RAEM que não utilizem redes ou que apenas utilizem redes cuja operacionalidade, protecção e segurança sejam garantidas por outras entidades públicas, nos termos das disposições legais orgânicas aplicáveis ou por despacho do Chefe do Executivo.

3.2. Operadores privados de infra-estruturas críticas.

Na sociedade contemporânea, vários serviços públicos importantes tendem a ser entregues à "exploração privada". Estes serviços passam a ser fornecidos por empresas ou entidades particulares, que, nessa medida, concorrem com as entidades públicas na prestação de serviços essenciais ao bem-estar e ao funcionamento sustentável da sociedade.

Nesse sentido, sugerimos que por "operadores privados de infra-estruturas críticas" se entendam as entidades particulares que:

- exploram actividades específicas e estabelecidas, de relevante interesse público, sob forma de concessão, licenciamento ou adjudicação de prestação de serviços;

- as sociedades de capitais exclusivamente públicos; e
- determinadas pessoas colectivas privadas qualificadas de utilidade pública administrativa por meio de diploma legal, com exclusão dos casos em que a actividade desenvolvida assim o justifique.

As referidas entidades são estabelecidas e exploradas nos termos dos regimes jurídicos existentes, compreendendo nomeadamente:

(1) Entidades estabelecidas e exploradas mediante um título de concessão, de licença ou de adjudicação de prestação de serviços à Administração: fornecimento e distribuição de água, electricidade e gás natural, abastecimento público grossista de combustíveis, tratamento de águas residuais e recolha e tratamento de resíduos, abastecimento público grossista de produtos alimentares sujeitos a controlos sanitários e fitossanitários, abate de animais em matadouros legais, portos e transportes maritimos, aeroporto, heliportos e transportes aéreos, transportes terrestres, difusão sonora e televisiva (com excepção da televisão por satélite e dos operadores cuja actividade se cinja à difusão de conteúdos de entretenimento), jogos de fortuna e azar em casinos;

(2) Entidades estabelecidas e exploradas mediante um título de licença administrativa: hospitais privados; sectores bancários, financeiro e segurador; operação das redes públicas de telecomunicações fixas ou móveis e prestação de serviços de acesso à *internet* (especificamente designados por operadores da rede pública; e outras entidades licenciadas nos domínios de actividades referidos no ponto (1) anterior;

(3) Sociedades de capitais exclusivamente públicos; e

(4) Pessoas colectivas qualificadas de utilidade pública administrativa por meio de diploma legal, com excepção daquelas cujas finalidades se cinjam às actividades humanitárias, assistenciais, educativas, culturais e/ou recreativas.

4. Entidades supervisoras do Governo

Um bom mecanismo de supervisão é factor determinante para uma efectiva prevenção dos ataques pela "Lei de Cibersegurança". Por isso, em cumprimento do princípio da "Simplicidade e eficácia do enquadramento institucional", sugerimos um enquadramento funcional de três níveis no que diz respeito ao sistema de supervisão de cibersegurança:

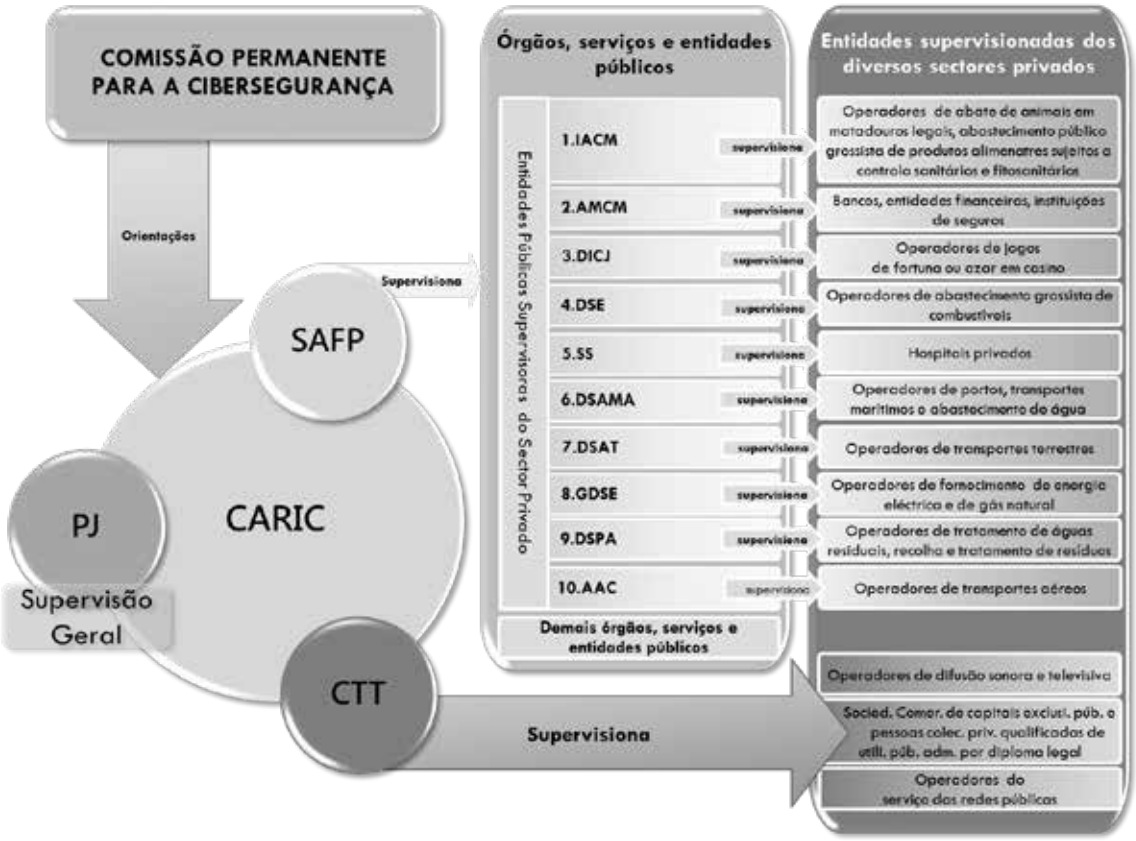
O primeiro nível: a **"Comissão Permanente para a Cibersegurança"**, órgão no topo hierárquico;

O segundo nível: **"Centro de Alerta e Resposta a Incidentes de Cibersegurança"**, órgão operacional e coordenador;

O terceiro nível: **"Entidades de supervisão por domínios de actividade"** *(vide o quadro abaixo).*

O sistema de supervisão de três níveis funciona organicamente, com uma conexão directa entre a estratégia e a execução, ligando os diferentes níveis, de modo a garantir uma supervisão eficaz.

ENQUADRAMENTO INSTITUCIONAL DE CIBERSEGURANÇA



4.1. A Comissão Permanente para a Cibersegurança

"A Comissão Permanente para a Cibersegurança" é um órgão decisório do Governo, que supervisiona macroscopicamente a situação da cibersegurança da RAEM em geral, e compete-lhe principalmente definir orientações, objectivos de ordem geral e de estratégias da cibersegurança; acompanhar e avaliar o desenvolvimento e funcionamento dos serviços e entidades públicas, bem como das entidades privadas, no âmbito da actividade de cibersegurança; apreciar e deliberar sobre o relatório geral de cibersegurança da RAEM; emitir orientações ao Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC), e às entidades de supervisão de cibersegurança.

A Comissão tem como presidente o Chefe do Executivo, como vice-presidente o Secretário para a Segurança, e como vogais os demais secretários do Governo e os dirigentes das entidades de supervisão de cibersegurança.

4.2. Centro de Alerta e Resposta a Incidentes de Cibersegurança

O CARIC é uma organização que serve principalmente para a concretização do trabalho de prevenção no âmbito da cibersegurança, nomeadamente a conexão entre os diferentes níveis, a transmissão de informações internas, e a comunicação interna e externa. Cabe à Polícia Judiciária, à Direcção dos Serviços de Administração e Função Pública e à Direcção dos Serviços dos Correios e Telecomunicação a operacionalidade do CARIC.

Para um funcionamento eficaz, o trabalho de supervisão no âmbito do cumprimento dos deveres da cibersegurança vai ser realizado pelo pessoal enviado pelos três serviços que, para além de exercerem as suas próprias funções, cooperam e comunicam.

A Polícia Judiciária assume funções de coordenação no funcionamento do CARIC que opera ininterruptamente 24 horas por dia. O CARIC, conforme a prática comum a nível internacional, vai monitorizar o tráfego de dados informáticos sob a forma de linguagem máquina, entre as redes dos operadores das infra-estruturas críticas e a internet, e, se necessário, supervisionar em tempo real a dimensão do fluxo dos dados e as características dos datagramas, etc., com a finalidade de prevenir, detectar e combater os ataques e invasões cibernéticos.

Compete ao CARIC:

1) Reagir a incidentes de cibersegurança, promover os deveres e medidas de cibersegurança, centralizar, para o efeito, os alertas de cibersegurança recebidos, coordenar a cooperação e acções adequadas entre os diversos intervenientes, cooperar com as entidades congéneres do exterior, de modo a evitar ou atenuar os

efeitos dos incidentes;

2) Definir e divulgar junto de todos os intervenientes no sistema de cibersegurança os modelos, as instruções e os procedimentos das acções de alerta e resposta aos incidentes, tendo em conta os objectivos e políticas preconizados pela Comissão Permanente, bem como as experiências bem conseguidas a nível internacional; e emitir, quando necessário, alertas sobre incidentes de cibersegurança;
3) Apresentar à Comissão Permanente um relatório geral de cibersegurança e prestar o apoio de que esta careça;
4) Prestar o apoio técnico necessário às entidades de supervisão e supervisionadas, para efeitos do cabal cumprimento das suas responsabilidades e deveres;
5) Promover acções de divulgação e sensibilização em matéria de cibersegurança.

4.3. Entidades supervisoras do Governo nos diversos domínios

De acordo com a sua definição, as "infra-estruturas críticas" são divididas em sector público e sector privado, por isso, o terceiro nível do sistema de supervisão - **"Entidades de supervisão em vários domínios"**, é também separado, correspondentemente, em duas partes:

- por um lado, cabe à Direcção dos Serviços de Administração e Função Pública supervisionar os órgãos e entidades públicos;

- por outro lado, compete a onze serviços públicos supervisionar os operadores das infra-estruturas críticas do sector privado.

A distribuição das tarefas de supervisão dos operadores privados é detalhada como segue (vide o quadro na página 11):

1) Os operadores de abate de animais em matadouros legais e de abastecimento público grossista de produtos alimentares sujeitos a controlos sanitários e fitossanitário, pelo Instituto para os Assuntos Cívicos e Municipais;
2) Os bancos, entidades financeiras e instituições de seguros, pela Autoridade Monetária de Macau;
3) Os operadores de jogos de fortuna ou azar em casinos, pela Direcção de Inspecção e Coordenação de Jogos;
4) Os operadores de abastecimento público grossista de combustíveis, pela Direcção dos Serviços de Economia;
5) Os operadores de portos e transportes marítimos e de abastecimento de água, pela Direcção dos Serviços de Assuntos Marítimos e de Água;
6) Os operadores de transportes terrestres, pela Direcção dos Serviços para os Assuntos de Tráfego;
7) Os hospitais privados, pelos Serviços de Saúde;

8) Os operadores de fornecimento e distribuição de electricidade e de gás natural, pelo Gabinete para o Desenvolvimento do Sector Energético;
9) Os operadores de tratamento de águas residuais e de recolha e tratamento de resíduos, pela Direcção dos Serviços de Protecção Ambiental;
10) Os operadores de redes públicas, os operadores de difusão sonora e televisiva, as sociedades comerciais de capitais exclusivamente públicos e as pessoas de utilidade pública administrativa referidas supra, na alínea (4) do n.° 3.2, pela Direcção dos Serviços de Correios e Telecomunicações.
11) Os operadores de transportes aéreos, pela Autoridade de Aviação Civil.

Compete às **"entidades de supervisão", nos respectivos domínios de competência**:

1) Definir o regime de gestão da cibersegurança dos operadores sujeitos à sua supervisão, designadamente no que respeita aos mecanismos e instrumentos de rotina de defesa contra ataques e invasões cibernéticos, tendo em conta as orientações preconizadas pela Comissão Permanente;
2) Colaborar com o CARIC, na definição das instruções de procedimentos de respostas a emergência e na implementação de tais procedimentos, quando ocorram incidentes;
3) Recolher os relatórios sobre a cibersegurança dos operadores sujeitos à sua supervisão, remetendo cópia dos mesmos ao CARIC;
4) Fiscalizar o cumprimento das regras de cibersegurança, nos termos legais.

5. Deveres legais

O regime de gestão preventiva da cibersegurança necessita de uma colaboração activa das respectivas instituições. Assim, é imprescindível definir os deveres aos quais devem estar sujeitos os operadores do sector privado e os operadores públicos das infra-estruturas críticas.

Sugerimos que os deveres dos operadores das infra-estruturas críticas sejam divididos, de acordo com a sua natureza, em quatro tipos:

1) Deveres de carácter orgânico;
2) Deveres de carácter procedimental, preventivo e reactivo;
3) Deveres de auto-avaliação e relato;
4) Deveres de colaboração.

Tendo em consideração a natureza específica das operadoras de rede e das entidades públicas e das suas actividades, propomos algumas especificidades de regime para elas, conforme mais detalhadamente se refere nos n.°s 5.5 e 5.6 do presente documento.

5.1. Deveres de carácter orgânico

Tendo em conta a confidencialidade e a sensibilidade da cibersegurança, "pessoal especializado" e "transmissão das informações com exactidão" constituem factores que devem ser considerados na estrutura orgânica dos operadores das infra-estruturas críticas, razão pela qual, sugerimos que os operadores privados tenham, no âmbito da respectiva organização, os seguintes deveres:

1) Criar unidades de gestão da cibersegurança e designar os respectivos responsáveis, aos quais cabe implementar, através da aplicação dos recursos humanos, financeiros, materiais e patrimoniais, medidas internas para protecção da segurança da rede;
2) Proceder à verificação de antecedentes (*vetting*) de idoneidade e experiência profissional dos responsáveis e técnicos em lugares-chave que operam as infra-estruturas críticas, solicitando obrigatoriamente, para esse efeito, parecer à Direcção da Polícia Judiciária;
3) Estabelecer mecanismos e meios para apresentar reclamações e denúncias relacionadas com a cibersegurança.

Em sede de verificação de antecedentes, considera-se que não possui idoneidade para assumir o cargo ou posição de responsável de cibersegurança a pessoa condenada, por sentença transitada em julgado, pela prática de qualquer dos crimes abaixo indicados:

(1) Por crime previsto na Lei n.° 2/2009 (Lei relativa à Segurança e Defesa do Estado);

(2) Por crime informático ou de falsificação de notação técnica, danificação ou subtracção de notação técnica, devassa da vida privada, aproveitamento indevido de segredo, violação de segredo de correspondência ou telecomunicações, ou de qualquer outro tipo de violação de segredo;

(3) Por qualquer outro crime punível com pena de prisão cujo limite máximo seja superior a 5 anos.

As sentenças proferidas por tribunal alheio ao sistema judiciário da RAEM são relevantes para efeitos de verificação de antecedentes acima referida, contanto que, no caso de crime punível com pena de prisão cujo limite máximo seja superior a 5 anos, a conduta em causa também constitua crime à luz da lei da RAEM.

5.2. Deveres de carácter procedimental, preventivo e reactivo

A cibersegurança depende crucialmente de um regime eficaz de gestão de informações diárias e de sistema de rede, de procedimentos operacionais, bem como das medidas de prevenção e de resposta às emergências. Para concretizar estes regime, procedimentos e medidas é imprescindível o cumprimento dos referidos deveres.

Por isso, sugerimos que os operadores das infra-estruturas críticas, em termos de procedimentos, prevenção e monitorização de incidentes de cibersegurança, bem como no âmbito de resposta às emergências, tenham os seguintes deveres:

1) Estabelecer um regime de gestão da cibersegurança e procedimentos operacionais internos;
2) Implementar, conforme o regime de gestão da cibersegurança e os circulares e outras instruções emitidos pelas entidades de supervisão, medidas internas de protecção, monitorização, alerta e resposta às emergências da cibersegurança, nomeadamente: a) prevenir que a rede e os dados que ali circulam sejam atingidos por incidentes ou actos não autorizados, tais como, o acesso, aquisição indevida, aditamento, utilização, alteração, controle, invasão, interferência, revelação, danificação ou destruição; b) monitorizar e efectuar registos do estado de funcionamento da rede, nomeadamente, armazenar e fornecer, em tempo oportuno, os registos de *web logs* nos termos previstos;
3) Informar o Centro de Alerta e Resposta a Incidentes de Cibersegurança da ocorrência de tais incidentes, dando conhecimento do facto à respectiva entidade de supervisão e iniciando, simultaneamente, as acções de resposta à emergência.

5.3. Deveres de auto-avaliação e relato

A fim de poder controlar a situação da implementação da cibersegurança e poder verificar se o trabalho preventivo dos diferentes âmbitos deram os resultados previstos, sugerimos que os operadores das infra-estruturas críticas tenham os seguintes deveres no âmbito de auto-avaliação e relato:

1) Proceder, com o próprio pessoal ou com a intervenção de entidades profissionais a quem deleguem, a avaliação, da segurança e dos eventuais riscos existentes na rede;
2) Submeter anualmente à entidade de supervisão à qual pertence um relatório sobre a cibersegurança, no qual deverão referir principalmente os eventuais incidentes de cibersegurança registados, os resultados da avaliação referida na alínea anterior e as medidas de melhoramento tomadas.

5.4. Dever de colaboração

Relativamente à prevenção e investigação de incidentes de cibersegurança, como as informações que se encontram na rede podem "desaparecer" rapidamente, são necessárias a recolha imediata e colaboração de diferentes partes, para conseguir recolhê-los.

Assim, sugerimos que os operadores das infra-estruturas críticas, bem como os respectivos administradores, gerentes ou mandatários tenham os seguintes deveres:

1) Facultar, na medida necessária à verificação do cumprimento dos deveres de carácter procedimental, preventivo e reactivo, a entrada dos representantes credenciados do Centro de Alerta e Resposta a Incidentes de Cibersegurança e das entidades de supervisão nas suas instalações, permitindo-lhes entrar no local de trabalho, e disponibilizar-lhes as informações solicitadas no âmbito das suas funções;
2) Prestar o apoio e a colaboração necessários para garantir a boa gestão da cibersegurança.

5.5. Deveres específicos dos operadores da rede pública

Os operadores da rede pública uma vez que são detentores de licença para operar a rede de telecomunicações fixa pública ou móvel e entidades que prestam serviço de acesso à internet, têm indubitavelmente um papel muito importante na cibersegurança. Por este motivo, para além dos deveres acima referidos, sugerimos que devem ainda:

1) Implementar o "*Real-Name System*": os operadores da rede pública ao celebrarem contratos com seus utentes e ao confirmarem a prestação de serviços de acesso à internet, serviços de registo de nomes de domínio, serviços das redes públicas de telecomunicações fixas ou móveis, aos utentes, devem solicitar os dados de

identificação verdadeiros;

2) Proceder à "conservação de registos "*Web logs*": ao disponibilizarem aos utentes serviço de acesso à internet, devem conservar durante um ano os registos de *Web Logs* das translações entre os endereços IP internet e os endereços das redes internas dos utentes.

5.6. Deveres dos operadores públicos das infra-estruturas críticas

Os operadores públicos das infra-estruturas críticas, na prática, são órgãos, serviços e entidades governamentais. As suas actividades, obviamente, estão relacionadas com os interesses públicos, e eles assumem a missão social de prestar serviços críticos.

Os operadores públicos estão obrigados, portanto, aos mesmos deveres essenciais a que estão os operadores privados, ou seja, precisam de cumprir todos os deveres de carácter procedimental, preventivo e reactivo, de auto-avaliação e relato e de colaboração. Quanto os deveres de carácter orgânico, como a criação de serviços públicos é feita de maneira muito cuidadosa e já existe um sistema público de reclamação e sugestões, bastará prever expressamente que os operadores públicos devem designar, de entre o pessoal da direcção ou equiparado, uma pessoa para assumir as funções de responsável pela cibersegurança, à qual cabe implementar medidas de protecção internas de cibersegurança através da aplicação de adequados recursos humanos, financeiros e materiais.

6. Incumprimento dos deveres e respectivas sanções administrativas e responsabilidades disciplinares

No contexto do regime jurídico em causa, sugerimos que, pelo incumprimento dos deveres de cibersegurança, não sejam aplicadas sanções penais, mas apenas sanções administrativas, nomeadamente pelas três seguintes razões:

1) O sistema de cibersegurança, na sua natureza, é um regime preventivo, no âmbito da gestão administrativa;

2) As infracções às disposições preventivas, geralmente, não são criminalizadas, ou seja, as mesmas não são punidas a título de crime;

3) Esta solução é compatível com o "princípio de intervenção mínima do Direito Penal", que constitui um princípio geral que caracteriza o sistema jurídico da RAEM.

Por esses motivos, propomos que o incumprimento dos deveres acima referidos, por acção ou omissão, constitua infracção administrativa e seja punida com multa, sem prejuízo da efectivação das responsabilidades penais previstas na demais legislação ou regulamentação.

Pelas infracções consideradas menos graves, prevê-se uma multa de 50.000 a 150.000 patacas; pelas infracções graves, uma multa de 150.000 a 5.000.000 patacas.

Àqueles que violem gravemente os deveres, ou seja, quando o incumprimento dos deveres possa causar danos ou prejuízos graves, poderão ser aplicadas separada ou cumulativamente as seguintes sanções acessórias: privação do direito à participação em concursos públicos, abertos por serviços e entidades públicas, para a aquisição de bens ou serviços, privação do direito aos subsídios ou benefícios concedidos por órgãos ou entidades públicos, e suspensão do efeito parcial ou total da autorização, licença, contrato de concessão ou alvará.

Em contrapartida, em determinadas situações consideradas de menor gravidade (quando o incumprimento dos deveres não constituir perigo substancial para a cibersegurança e não for caso de reincidência), a sanção poderá resumir-se a uma advertência, se o infractor sanar a irregularidade dentro do prazo indicado pela autoridade.

Os operadores privados de infra-estruturas críticas deverão responder institucionalmente, a título principal, pela infracções cometidas no âmbito das suas organizações, independentemente das acções que entendam desenvolver, contra as pessoas envolvidas na situação de infracção, e independentemente da categoria em que estas pessoas envolvidas se encontrem na instituição e da respectiva relação funcional ou de emprego com o operador.

Relativamente aos operadores públicos das infra-estruturas críticas, os funcionários responsáveis pelos incumprimentos dos deveres de cibersegurança, a

título de dolo ou negligência, serão sujeitos a responsabilidade disciplinar. Se estiver em causa incumprimento de algum dos deveres de cibersegurança essenciais *(ou seja, dos deveres de carácter procedimental, preventivo e reactivo),* a pena disciplinar não poderá, em regra, ser inferior a suspensão de exercício de funções (de 10 a 240 dias), podendo, nos casos graves, culminar na pena de demissão.

7. Ponderações especiais sobre a data da entrada em vigor

Visto que o regime jurídico preventivo da cibersegurança é um sistema completamente novo, sugerimos que, conforme a forma habitual de produção legislativa, seja fixada uma data que permite um espaço de tempo razoável para a entrada em vigor da proposta de lei, isto é, o mesmo entrará em vigor 30 dias após a sua publicação.

Todavia, considerando que a "Lei da Cibersegurança" e os serviços públicos da rede estão intimamente ligados, para não provocar um impacto aos operadores da rede pública, propomos que seja estipulada uma outra data de entrada em vigor exclusivamente para os dois deveres especiais dos operadores da rede — "*Real-Name System*" e conservação de *Web Logs*.

Esta norma visará permitir que os operadores possam, durante o *vacatio legis* (período de vacância), fazer preparativos e adaptações às novas disposições, evitando, o mais possível, grande impacto para a venda no mercado dos cartões telefónicos pré-pagos e cartões para o acesso à internet, no sentido de não afectar os negócios nem os rendimentos dos operadores, e que, no período de vacância, possam vender, o maior número possível dos restantes cartões que não exigem o registo dos dados pessoais do utente.

8. Regulamentação

De acordo com a Lei n.º 13/2009 (Regime jurídico de enquadramento das fontes normativas internas), o Governo pode regular a sua estrutura orgânica mediante regulamentos administrativos. Assim, através dos regulamentos administrativos complementares, serão reguladas as competências e o funcionamento da Comissão Permanente para a Cibersegurança e do Centro de Alerta e Resposta a Incidentes de Cibersegurança, e serão definidos os domínios privados sujeitos à supervisão, bem como as entidades públicas supervisoras.

Este modelo de regulamento é também dotado de carácter pragmático, permitindo a actualização e os ajustamentos, quando necessário, em matérias de designação das entidades supervisoras, suas competências e funcionamento e os domínios privados sujeitos à supervisão.

Tabela para sugestões e opiniões acerca da proposta da "Lei de Cibersegurança"

Dados básicos do opinante/proponente
Nome do opinante/proponente /Designação da entidade:
Actividade do sector ligado às infra-estruturas críticas ou de outros sectores (por exemplo, fornecimento da electricidade):
Declaração de confidencialidade: Por favor assinale com o sinal ✓ a quadrícula caso deseje manter a sua opinião ou sugestão em segredo ----------☐
Data de entrega:

Capítulos e secções focalizados na opinião ou sugestão	**Opinião ou sugestão**
1. Criação do sistema de protecção da cibersegurança	
2. Definições relativas às infra-estruturas críticas e à cibersegurança	
3. Âmbito de aplicação do sistema de protecção da cibersegurança	
3.1. Operadores públicos das infra-estruturas críticas	
3.2. Operadores privados das infra-estruturas críticas	
4. Entidades supervisoras do Governo	
4.1. Comissão Permanente para a Cibersegurança	
4.2. Centro de Alerta e Resposta a Incidentes de Cibersegurança	
4.3. Entidades supervisoras do Governo nos diversos domínios	
5. Deveres legais	
5.1. Deveres de carácter orgânico	
5.2. Deveres de carácter procedimental, preventivo e reactivo	
5.3. Deveres de auto-avaliação e relato	
5.4. Dever de colaboração	

5.5. Deveres específicos dos operadores da rede pública	
5.6. Deveres dos operadores públicos das infra-estruturas críticas	
6. Incumprimento dos deveres e respectivas sanções administrativas e responsabilidades disciplinares	
7. Ponderações especiais sobre a data da entrada em vigor	
8. Regulamentação	
9. Outras matérias sobre a cibersegurança não mencionadas no documento de consulta	

Observações:

- Este formulário serve apenas de referência e destina-se a facilitar a análise e organização durante o preenchimento de opiniões ou sugestões;
- Se não houver espaço suficiente, por favor preencha segundo a ordem dos títulos em folha separada, marcando o respectivo capítulo ou secção e a página em que consta;
- Agradecemos que o conteúdo seja expresso de forma directa e sucinta quanto possível.