LEI DA CIBERSEGURANÇ A

RELATÓ RIO FINAL DA CONSULTA PÚ BLICA

REGIÃ O ADMINISTRATIVA ESPECIAL DE MACAU

ANO 2018

Fonte das opiniões

1. Os sectores profissionais / institucionais

De acordo com as definições do documento de consulta, "Infra-estruturas críticas" são patrimónios, sistemas e redes que se consideram relevantes para o interesse da sociedade e para o seu funcionamento normal; "Operadores das infra-estruturas críticas" são entidades públicas ou privadas que operam as infra-estruturas críticas ou que prestam serviços ligados às mesmas.

(1) **Operadores públicos de infra-estruturas críticas:** incluem órgãos, serviços e entidades públicos;

(2) **Operadores privados de infra-estruturas críticas:** incluem operadores de abate de animais em matadouros legais, abastecimento público grossista de produtos alimentares sujeitos a controlos sanitários e fitossanitários; bancos, entidades financeiras e instituições de seguros; operadores de jogos de fortuna ou azar em casinos; operadores de abastecimento público grossista de combustíveis; hospitais privados; operadores de portos, transportes marítimos e de abastecimento de água; operadores de transportes terrestres; operadores de fornecimento e distribuição de energia eléctrica e de gás natural; operadores de tratamento de águas residuais, recolha e tratamento de resíduos; operadores de transportes aéreos; operadores de difusão sonora e televisiva, sociedades comerciais de capitais exclusivamente públicos e pessoas colectivas privadas qualificadas de utilidade pública administrativa por diploma legal; operadores de redes públicas.

2. O público

Critérios de classificação de síntese de opiniões e de opiniões

1. **"Síntese das opiniões"** entende-se por "síntese das opiniões" o resumo crítico das opiniões recolhidas, relativas aos diversos tópicos, centrado sobre aquelas que suscitaram maior atenção ou a que foi conferida maior importância.

2. **"concorda"** entende-se que "concorda" quem, no texto original das opiniões, manifestou claramente a sua concordância com o conteúdo dos capítulos e subcapítulos do documento de consulta *(ou seja, nas opiniões surgiram as expressões de "concordo", "a favor", "reconhecimento", "consentimento" etc.)* e ainda quem, mesmo não usando tais expressões, se manifestou de tal forma que é possível retirar do seu texto o sentido de concordância.

3. **"não concorda"** entende-se que "não concorda" quem, no texto original das opiniões, manifestou claramente a sua discordância com o conteúdo dos capítulos e subcapítulos do documento de consulta *(ou seja, nas opiniões apareceram as expressões "não concordo", "contra", "não consentimento", "não deve fazer isso" etc.,)* e ainda quem, mesmo não usando tais expressões, se manifestou de tal forma que é possível retirar do seu texto o sentido de discordância.

4. **"outras opiniões"** entende-se por "outras opiniões" aquelas em que, no texto original, se levantaram outras opiniões ou sugestões em relação ao conteúdo dos capítulos e subcapítulos do documento de consulta, mas sem ser possível concluir se há concordância ou discordância com aquele conteúdo

5. **"nulas"** entende-se por "nulas" as opiniões em que, no respectivo texto original, são expressas palavras insultuosas e gíria ou incompreensíveis *(ex. símbolos, caracteres ilegíveis, poesias não relacionadas, etc.)*

Nas partes de "breve conclusão" e "conclusão" dos diversos capítulos, quanto às manifestações aos tópicos, obtém-se através de somar a percentagem de "concorda" e "não concorda" a conclusão sobre **concordância na generalidade** ou **discordância na generalidade**

Relatório Final da Consulta Pública da "Lei da Cibersegurança"

Índice

INTRODUÇÃO

A "Lei da Cibersegurança" será a base legal do sistema de segurança das redes informáticas de Macau e definirá os deveres e as responsabilidades dos diversos operadores das infra-estruturas críticas de Macau e da sociedade, bem como o trabalho de segurança da rede, no âmbito de gestão administrativa, incluindo em termos de avaliação de risco, alarme prévia, prevenção, supervisão, e outros trabalhos de contingência, etc., para a construção de um sistema de gestão de controlo da segurança de rede eficaz, com vista a melhorar a capacidade de prevenção e resposta de segurança cibernética de Macau e melhor proteger a segurança da Região Administrativa Especial de Macau (RAEM) e do Estado.

O Governo da RAEM procedeu à consulta pública sobre a "Lei da Cibersegurança", que decorreu entre os dias 11 de Dezembro de 2017 e 24 de Janeiro de 2018, com uma duração de 45 dias. Durante este período, tendo em vista aperfeiçoar o projecto de lei e planear conjuntamente o estabelecimento dum sistema de protecção no âmbito de cibersegurança, em conformidade dos desejos dos cidadãos e das necessidades reais do desenvolvimento de Macau, foi efectuada a discussão em ampla escala junto dos diversos sectores da sociedade, visando convergir para um consenso da sociedade e lançar um sólido alicerce jurídico para estabelecer um sistema de segurança cibernética.

Esta consulta pública, cuja coordenação coube ao Gabinete do Secretário para a Segurança, foi promovida em conjunto por 13 serviços, órgãos e entidades públicos, incluindo a Direcção dos Serviços da Administração e Função Pública, a Direcção dos Serviços de Economia, a Direcção dos Serviços de Assuntos Marítimos e de Água, a Direcção dos Serviços para os Assuntos de Tráfego, o Gabinete para o Desenvolvimento do Sector Energético, a Direcção dos Serviços de Protecção Ambiental, Autoridade de Aviação Civil, a Autoridade Monetária de Macau, Direcção de Inspecção e Coordenação de Jogos, o Instituto para os Assuntos Cívicos e Municipais, Serviços de Saúde, a Direcção dos Serviços de Correios e Telecomunicações e a Polícia Judiciária. Acresce que foram dadas as opiniões e a participação em sessões de consulta pelo Gabinete para a Protecção de Dados Pessoais, ainda por acima, no processo da elaboração do projecto, o Conselho Consultivo da Reforma Jurídica e a Direcção dos Serviços de Assuntos de Justiça procederam a discussões tendo apresentado nelas opiniões nas vertentes política e jurídica.

Após o termo das actividades de consulta, os 14 serviços, órgãos e entidades públicos acima mencionados avançaram logo, em diversos aspectos, ao tratamento das opiniões e sugestões recolhidas pelas diversas vias, durante o período de consulta, e produziram o presente relatório final.

O presente relatório final é dividido em 4 partes: na 1.ª parte consta a descrição geral dos trabalhos de consulta; na 2.ª parte constam a síntese, análise e breve conclusão das opiniões relativas ao documento de consulta; na 3.ª parte constam as opiniões e sugestões sobre a matéria não mencionada no documento da consulta; na 4.ª parte, é exposta a conclusão.

Parte I

Situação geral do trabalho da consulta

No período de consulta, o Governo da RAEM procedeu, por várias vias, a actividades de divulgação para apresentar o conteúdo da Lei da Cibersegurança aos sectores da sociedade, nomeadamente através da organização de conferência de imprensa, de sessões de consulta destinadas ao diversos sectores relacionados e ao público, de *site* temático na página electrónica, de divulgação nos *media* e nas plataformas das redes sociais, de distribuição de documento da consulta e folhetos, etc., tendo activamente recolhido as opiniões dos sectores e da sociedade em geral, e tendo efectuado análises, por via de *brainstorming*, para melhorar o conteúdo do projecto da lei.

1. Distribuição do documento de consulta

Durante o período de consulta da Lei da Cibersegurança, foram disponibilizados 2.400 exemplares do documento de consulta e 2.700 panfletos ao público, em diversos locais, nomeadamente no Gabinete do Secretário para a Segurança, na Direcção dos Serviços da Administração e Função Pública, na Direcção dos Serviços de Assuntos de Justiça, na Polícia Judiciária, no Centro de Informações do Governo, no Centro de Serviços da RAEM e no Centro de Prestação de Serviços ao Público da Zona Central e das Ilhas. Além disso, para facilitar a consulta pelos cidadãos, o documento de consulta da Lei da Cibersegurança foi também carregado para o *site* temático do Gabinete do Secretário para a Segurança (www.gss.gov.mo/pt/ciberseg).

2. Promoção por via dos *media*

A fim de obter melhor entendimento da sociedade sobre o objectivo e o conteúdo da legislação da Lei da Cibersegurança, além do *site* temático, foram também produzidos na consulta vídeos elucidativos, anúncios sonoros e infografias simples e fáceis de entender, cujo conteúdo está dividido em 4 aspectos: apresentação da consulta pública, "a Salvaguarda da segurança social - Lei da Cibersegurança", gestão da segurança da rede e deveres e responsabilidades da cibersegurança, tendo sido efectuadas amplas divulgações através de transmissão nos canais televisivos, na rádio, no interior dos autocarros de transporte público, bem como divulgadas as informações das actividades da consulta junto da sociedade, através das novas plataformas de redes sociais, tais como *Facebook* e *Wechat*, entre outros.

Durante o período de consulta, o Gabinete do Secretário para a Segurança efectuou, no total, 7 comunicados de imprensa para que o público possa conhecer atempadamente as notícias sobre a consulta, ao mesmo tempo que os serviços governamentais relacionados também acompanhavam atentamente notícias transmitidas pelos diversos meios de comunicação social, incluindo as reportagens e os comentários sobre a "Lei da Cibersegurança" emitidas pelo *media* tradicionais e pelas plataformas de redes sociais, com vista ao conhecimento da evolução da percepção pública a esse respeito.

Os representantes do Governo também participaram em programas de comentários noticiosos organizados pelos diversos *media*, trocando opiniões directamente com os cidadãos sobre a "Lei da Cibersegurança". Em 15 de Dezembro de 2017, participaram nos programas "*Call in Macau*", do Macau Lotus TV; em 19 de Dezembro, Macau Fórum da TDM; e no dia 17 de Janeiro de 2018, assistiram ao programa "*Macau Fórum*", da Rádio Macau.

3. Realização de várias sessões de consulta

Durante o período de consulta, realizaram-se, no total, 8 sessões de consulta, entre as quais 5 sessões destinadas aos serviços públicos e representantes dos operadores das infra-estruturas críticas e 3 destinadas aos cidadãos de Macau. As sessões foram activamente participadas por cerca de 600 pessoas, tendo, durante a mesma, sido recolhidas opiniões de muitos cidadãos e representantes dos sectores relacionados, as quais contribuíram de forma valiosa, positiva, para optimizar o conteúdo do projecto de lei.

Sessões de Consulta	Data	Destinatário
Sessões de consulta sectorial	11/Dez/2017	Serviços, órgãos e entidades públicos
	13/Dez/2017	Operadores de abastecimento grossista de combustíveis; os operadores de portos, transportes marítimos e abastecimento de água; os operadores de transportes terrestres; operadores de transportes aéreos; os operadores de fornecimento e distribuição de energia eléctrica e de gás natural; os operadores de tratamento de águas residuais, recolha e tratamento de resíduos;
	14/Dez/2017	Bancos, entidades financeiras e instituições de seguros;

Sessões de Consulta	Data	Destinatário
	15/Dez/2017	Operadores de jogos de fortuna ou azar em casinos;
	3/Jan/2018	Operadores de abate de animais em matadouros legais, abastecimento público grossista de produtos alimentares sujeitos a controlos sanitários e fitossanitários; os hospitais privados; os operadores de difusão sonora e televisiva; os operadores de redes públicas; sociedades comerciais de capitais exclusivamente públicos e pessoas colectivas privadas qualificadas de utilidade pública administrativa por diploma legal;
Sessões de consulta destinada ao Público	5/Jan/2018	Público e órgãos de comunicação social
	13/Jan/2018	
	15/Jan/2018	

4. Perguntas e respostas frequentes

A fim de permitir que a sociedade se aperceba correctamente da intenção legislativa da "Lei da Cibersegurança", o Gabinete do Secretário para a Segurança, de acordo com o conteúdo de perguntas e respostas dos participantes de consulta e as dúvidas ou opiniões apresentadas da sociedade em relação à "Lei da Cibersegurança", publicou, durante o período de consulta, um conjunto de perguntas e respostas frequentes, tendo sucessivamente efectuado a respectiva actualização e adicionado as informações complementares. As perguntas e respostas encontram-se disponíveis no *site* temático da página electrónica e as respectivas informações foram divulgadas junto dos cidadãos através da coluna "Conhecer melhor a cibersegurança", constante na plataforma de *Wechat*, a fim de dissipar as dúvidas do público.

5. Recolha de opiniões

Durante o período de consulta pública, as entidades supervisoras listadas na página 13 do documento da consulta, relativa ao "Enquadramento Institucional de Cibersegurança", convidaram os respectivos operadores de infra-estruturas críticas a apresentarem opiniões por escrito em relação ao conteúdo do documento de consulta. Durante o período de consulta, foram registadas 144 opiniões por escrito apresentadas oficialmente pelos serviços públicos e pelas entidades supervisionadas - operadores

privados das infra-estruturas críticas; 43 intervenientes fizeram a sua intervenção no decurso das 5 sessões de consulta sectorial.

Além disso, foram recolhidas 31 opiniões por escrito e 449 opiniões por via electrónica, através do preenchimento directo na coluna de opiniões constante no *site* temático, pelo público, e 49 participantes fizeram a sua intervenção no decurso das 3 sessões de consulta destinadas ao público.

<table>
<tr><th colspan="2">Origem das opiniões</th><th>Canais de recolha</th><th colspan="3">N.º de opiniões</th><th>Total</th></tr>
<tr><td rowspan="4">Sectorial</td><td rowspan="2">Serviços Públicos</td><td>Por escrito</td><td>36</td><td rowspan="2">38</td><td rowspan="4">187</td><td rowspan="5">716</td></tr>
<tr><td>Sessões de consulta</td><td>2</td></tr>
<tr><td rowspan="2">Entidades supervisionadas - operadores privados das infra-estruturas críticas</td><td>Por escrito</td><td>108</td><td rowspan="2">149</td></tr>
<tr><td>Sessões de consulta</td><td>41</td></tr>
<tr><td colspan="2" rowspan="3">Público</td><td>Por escrito</td><td>31</td><td colspan="2" rowspan="3">529</td></tr>
<tr><td>Site temático</td><td>449</td></tr>
<tr><td>Sessões de consulta</td><td>49</td></tr>
</table>

Nas 716 opiniões[1] recolhidas através de diferentes canais, foram expressas 3.081 opiniões temáticas de acordo com a matéria concretamente especificada nos capítulos e subcapítulos, sendo que os temas que mais preocupações suscitaram foram, principalmente, os seguintes: criação do sistema de protecção da cibersegurança *(intenção legislativa);* destinatários de aplicação do sistema de protecção da cibersegurança *(designadamente o âmbito de definição dos operadores privados das infra-estruturas críticas);* composição e competência da Comissão Permanente para a Cibersegurança e do Centro de Alerta e Resposta a Incidentes de Cibersegurança; e deveres específicos dos operadores de rede pública (designadamente, deveres de "*Real name system*" e "conservação dos registos de *Web logs*", entre outros conteúdos).

[1] De acordo com o critério estabelecido, uma das 716 opiniões foi considerada "nula".

Distribuição dos temas em destaque

Temas dos capítulos e subcapítulos	N.º de opiniões	N.º de opiniões recolhidas através de diferentes canais		
		Por escrito	*Site* temático	Consulta
1. Criação do sistema de protecção da cibersegurança	355	65	259	31
2. Definições relativas às infra-estruturas críticas e à cibersegurança	158	48	104	6
3. Âmbito de aplicação do sistema de protecção da cibersegurança	---	---	---	---
3.1 Operadores públicos das infra-estruturas críticas – órgãos, serviços e entidades públicos	169	34	134	1
3.2 Operadores privados das infra-estruturas críticas	235	51	179	5
4. Entidades supervisoras do Governo	---	---	---	---
4.1 "Comissão Permanente para a Cibersegurança"	229	36	185	8
4.2 "Centro de Alerta e Resposta a Incidentes de Cibersegurança"	238	56	175	7
4.3 Entidades supervisoras do Governo nos diversos domínios	164	40	114	10
5. Deveres legais	---	---	---	---
5.1 Deveres de carácter orgânico	182	103	66	13
5.2 Deveres de carácter procedimental, preventivo e reactivo	192	74	108	10
5.3 Deveres de auto-avaliação e relato	195	87	98	10
5.4 Dever de colaboração	176	57	113	6
5.5 Deveres específicos dos operadores da rede pública	243	70	140	24
5.6 Deveres dos operadores públicos das infra-estruturas críticas	64	31	30	3
6. Incumprimento dos deveres e respectivas sanções administrativas e responsabilidades disciplinares	173	66	106	1
7. Ponderações especiais sobre a data da entrada em vigor	146	60	85	1
8. Regulamentação	28	20	8	0
9. Outros assuntos sobre cibersegurança não referidos no presente documento de consulta	143	32	96	15
Total:	**3.081**	**930**	**2.000**	**151**

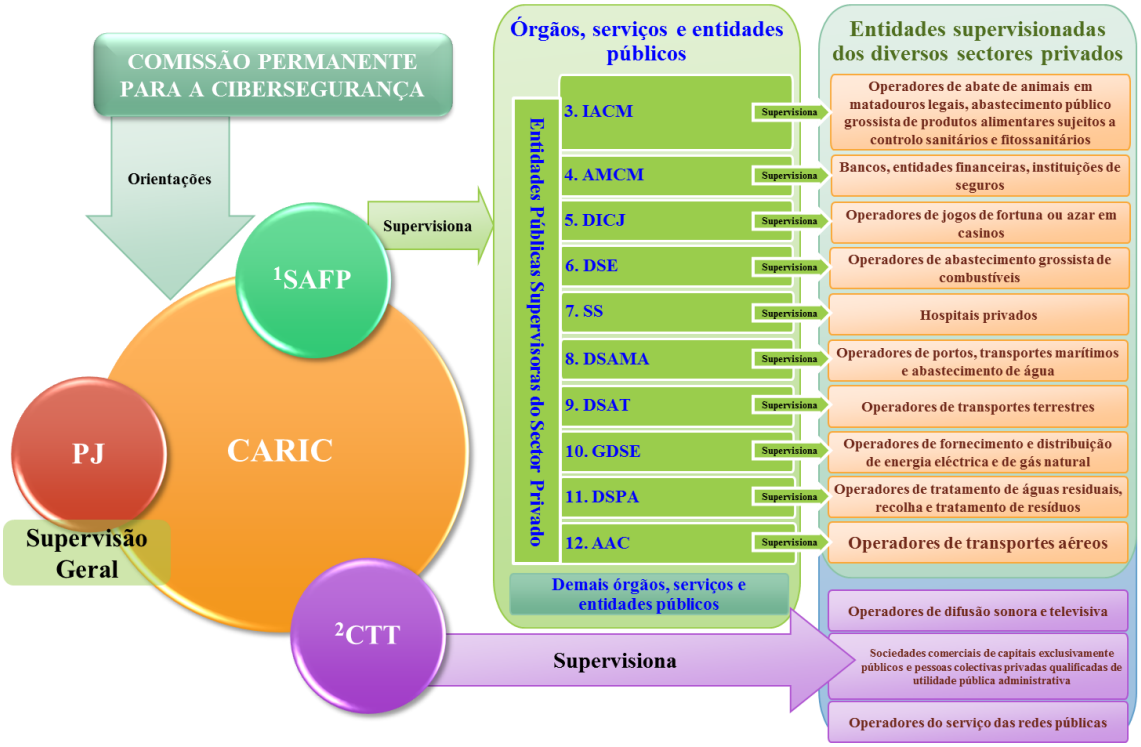

1. Criação do sistema de protecção da cibersegurança
355
4.2. Centro de Alerta e Resposta a Incidentes de Cibersegurança
238
3.2. Operadores privados das infra-estruturas críticas
235
5.5. Deveres específicos dos operadores da rede pública
234
4.1. Comissão Permanente para a Cibersegurança
229
5.3. Deveres de auto-avaliação e relato
195
5.2. Deveres de carácter procedimental, preventivo e reactivo
192
5.1. Deveres de carácter orgânico
182
5.4. Dever de colaboração
176
6. Incumprimento dos deveres e respectivas sanções administrativas e responsabilidades disciplinares
173
3.1. Operadores públicos das infra-estruturas críticas
169
4.3. Entidades supervisoras do Governo nos diversos domínios
164
2. Definições relativas às infra-estruturas críticas e à cibersegurança
158
7. Ponderações especiais sobre a data da entrada em vigor
146
9. Outros assuntos sobre cibersegurança não referidos no presente documento de consulta
143
5.6. Deveres dos operadores públicos das infra-estruturas críticas
64
8. Regulamentação
28

Parte II

Síntese, análise e breve conclusão das opiniões relativas ao documento da consulta

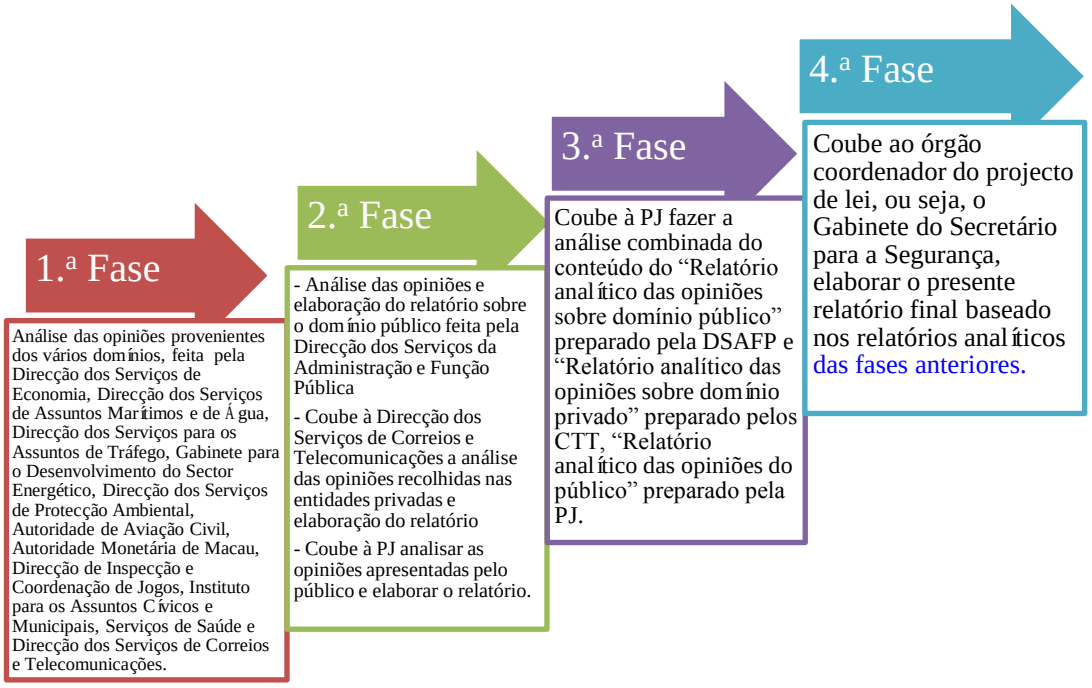
Dado que a "Lei da Cibersegurança" tem uma amplitude muita extensa na sociedade, envolvendo as actividades de 12 infra-estruturas críticas e as respectivas entidades supervisoras *(vide o esquema abaixo indicado)*, para poder fazer uma análise apropriada das opiniões recolhidas e ponderar devidamente a situação real da actividade desenvolvida pelos diversos sectores e em conformidade com o plano e a organização da consulta pública da "Lei da Cibersegurança", a análise das opiniões foi efectuada em 4 fases.

Enquadramento Institucional da Cibersegurança



(Vide o "Enquadramento Institucional da Cibersegurança" na página 13 do documento de consulta)

Procedimentos de trabalho da análise das opiniões

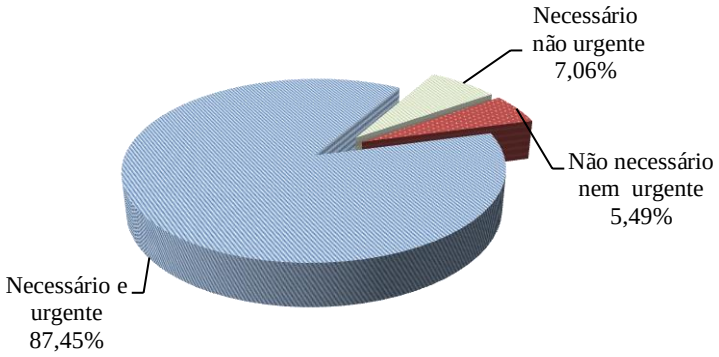


1. Criação do sistema de protecção da cibersegurança

O documento da consulta pública revela a necessidade de criar um sistema de gestão administrativa que visa proteger a cibersegurança da RAEM, definindo os deveres e as responsabilidades dos operadores das infra-estruturas críticas. A "Lei da Cibersegurança" é um diploma que visa a "protecção", "prevenção" e "gestão"; quanto aos ilícitos criminais que envolvem as áreas de *internet*, informações e computadores mantêm-se regulados na "Lei de Combate à Criminalidade Informática".

Relativamente a este assunto, foram recolhidas 241 opiniões que consideram que é necessário estabelecer o sistema de protecção da cibersegurança, 14 opiniões divergentes considerando desnecessário o estabelecimento do referido sistema, e registam-se ainda outras 100 opiniões, provenientes dos sectores e do público contendo sugestões relacionadas com a regulamentação das instruções a implementar no futuro, após a criação deste sistema, e dos respectivos regimes.

Opiniões	Necessário e urgente		Necessário mas não urgente		Não necessário nem urgente	
	Sector	**Público**	**Sector**	**Público**	**Sector**	**Público**
N.º	21	202	7	11	0	14
Percentagem	87,45%		7,06%		5,49%	



- **Síntese das opiniões**

Os representantes dos sectores, na generalidade, consideram que a cibersegurança é algo muito importante para a segurança e o funcionamento normal dos seus sistemas informáticos; por outro lado, a popularização gradual do uso das tecnologias informáticas pelas diversas camadas sociais e os ataques cibernéticos ocorrem frequentemente em todo o mundo, pelo que a criação do sistema de protecção da cibersegurança irá contribuir para prevenir e responder a eventuais incidentes que possam ocorrer em Macau, salvaguardando os direitos e interesses legítimos dos cidadãos.

O público, na generalidade, concorda com o estabelecimento do sistema de protecção da cibersegurança em Macau e algumas pessoas consideram que, com o desenvolvimento de Macau como "cidade inteligente" e a popularização dos pagamentos electrónicos, a criação do sistema de protecção da cibersegurança poderá ajudar Macau a prevenir os ataques cibernéticos que possam causar impactos negativos no funcionamento da sociedade; assim, o público concorda que o Governo proceda, o mais rápido possível, ao aperfeiçoamento das respectivas leis para proteger a população, especialmente para resolver o problema da devassa fácil das informações pessoais.

Uma minoria de opiniões (14 opiniões), provenientes do público, que discordam com a criação deste sistema, consideram que já existe actualmente em Macau a "Lei de Combate à Criminalidade Informática" para lidar com os ataques dos *hackers*, suscitando a preocupação de que o Governo possa aproveitar o estabelecimento da "Lei da Cibersegurança" para legalizar a vigilância cibernética, a qual poderá prejudicar os direitos dos cidadãos, nomeadamente a liberdade de expressão e o sigilo das comunicações.

Análise e resposta

A "Lei da Cibersegurança", de acordo com a intenção legislativa subjacente, visa constituir, sempre tendo em conta a "salvaguarda da segurança da população e respeito da privacidade pessoal", um sistema de gestão eficaz e destinado às infra-estruturas críticas, para prevenir e reduzir um eventual impacto na sociedade de Macau resultante de ataques cibernéticos.

A "Lei da Cibersegurança" tem como objecto as medidas preventivas (a tomar *a anteriori*, portanto) que visam a gestão preventiva da cibersegurança das infra-estruturas críticas, sendo que as mesmas não intervirão nem prejudicarão os direitos fundamentais dos residentes, nomeadamente a liberdade de expressão, a privacidade pessoal e a liberdade de imprensa. A "Lei de Combate à Criminalidade Informática" é uma lei penal relativa aos crimes informáticos e cibernéticos, ou seja, as diligências de investigação criminal são efectuadas após a prática dos crimes. Estas diligências, quando intervêm no conteúdo de comunicações, devem ser realizadas rigorosamente conforme os dispostos no artigo 32.º da Lei Básica e no artigo 164.º do Código de Processo Penal.

- **Síntese das opiniões**

Houve cidadãos que propõem ao Governo tomar como referências as experiências da criação do regime e da legislação dos países e regiões avançados na criação do sistema de protecção da cibersegurança em Macau.

Análise e resposta

No processo da concepção do enquadramento geral da cibersegurança sugerido no documento de consulta, já foi realizado um estudo comparativo e tomado como referência os regimes jurídicos do Interior da China e de outros países e regiões, tendo-se ainda em consideração as situações reais. No futuro, com a entrada em vigor desta lei, o Governo irá acompanhar de perto as

actualidades do trabalho da protecção da cibersegurança do mundo, bem como proceder atempadamente à revisão e à actualização, para que este se adapte ao desenvolvimento acelerado da tecnologia informática e às sucessivas alterações do ambiente da rede.

Breve conclusão

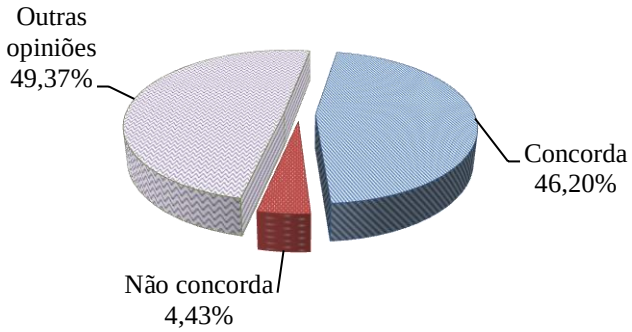
Mais de 87% das opiniões, quer dos sectores, quer do público, consideram que é necessário e urgente estabelecer um sistema de protecção da cibersegurança, apontando que a cibersegurança se configura como pressuposto e garantia da segurança pública e pessoal, pelo que a RAEM se obriga a criar um bom sistema de gestão preventivo, mediante acto legislativo, no intuito de assegurar o normal funcionamento dos sistemas da rede e proteger a confidencialidade e a integridade dos dados da rede.

2. Definição das infra-estruturas críticas e da cibersegurança

O documento de consulta propõe a definição dos conceitos essenciais da "Lei da Cibersegurança", nomeadamente as "infra-estruturas críticas", os "operadores das infra-estruturas críticas", a "rede", os "dados da rede", a "cibersegurança" e os "incidentes da cibersegurança".

Relativamente a este assunto, foram recolhidas 73 opiniões concordantes e 7 opiniões discordantes; outras 78 opiniões apresentaram sugestões concretas sobre os conteúdos indefinidos no documento de consulta.

Opiniões	Concorda		Não concorda		Outras
	Sector	Público	Sector	Público	
N.º	27	46	0	7	78
Percentagem	46,2%		4,43%		49,37%



- **Síntese das opiniões**

  Os sectores e o público propõem que sejam feitas definições mais pormenorizadas, e através dessas definições claras, definir explicitamente o âmbito da supervisão da "Lei da Cibersegurança".

  Análise e resposta

  Após a análise das opiniões recolhidas, o Governo introduz alterações e ajustamentos a algumas definições do documento de consulta, tais como a redefinição dos termos da "cibersegurança" e dos "incidentes da cibersegurança", bem como a introdução dos "actos não autorizados", para melhor definir o âmbito da "cibersegurança".

- **Síntese das opiniões**

  Os sectores e o público propõem que, acerca dos conteúdos indefinidos no documento de consulta (por exemplo, moeda digital), devem proceder-se à definição e supervisão.

  Análise e resposta

  Relativamente aos conteúdos indefinidos no documento de consulta, se houver disposições relevantes em outras leis existentes, não há necessidade nem é conveniente repetir estas disposições na "Lei da Cibersegurança". É de salientar que, uma vez que a "Lei da Cibersegurança" é uma lei de gestão administrativa que abrange várias áreas, deve ter uma ampla aplicabilidade, não sendo apropriado, portanto, proceder-se à definição e supervisão de um determinado conteúdo, muito especificado, nas disposições legais.

Breve conclusão

Os sectores e o público concordam, na generalidade, com a "definição das infra-estruturas críticas e da cibersegurança", tendo-se registado aproximadamente 50% das outras opiniões que propõem principalmente ao Governo para proceder à definição de outros conteúdos.

Após a análise das opiniões recolhidas, o Governo vai introduzir alterações e ajustamentos adequados às definições mencionadas no documento de consulta para as tornar mais claras e precisas, de forma a eliminar as dúvidas dos sectores e da população e lançar o alicerce mais sólido para a execução eficaz no futuro do projecto de lei.

3. Âmbito de aplicação do sistema de protecção da cibersegurança (os operadores das infra-estruturas críticas)

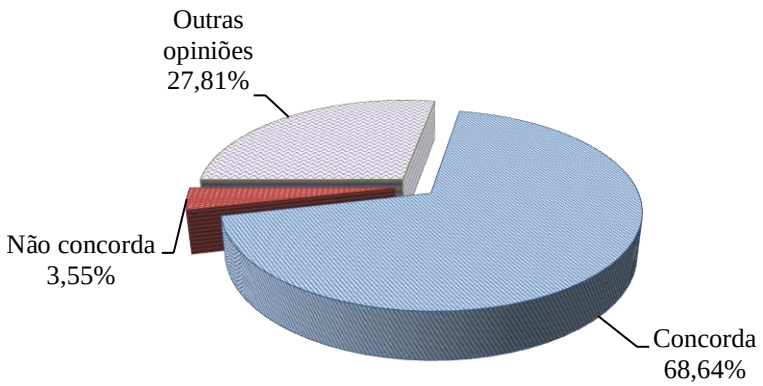
Os destinatários do sistema de protecção da cibersegurança são os "operadores das infra-estruturas críticas", que compreendem dois sectores - público e privado. Os "operadores das infra-estruturas críticas" são responsáveis pela segurança da rede das "infra-estruturas críticas", pelo que o seu papel é particularmente importante.

3.1 Os operadores públicos das infra-estruturas críticas – órgãos, serviços e entidades públicos

O documento de consulta propõe que os operadores públicos das infra-estruturas críticas integrem todos os órgãos, serviços e entidades públicos.

No que diz respeito ao âmbito de aplicação dos "operadores públicos das infra-estruturas críticas", foram recolhidas 116 opiniões concordantes e 6 opiniões discordantes, tendo sido recolhidas outras 47 opiniões que levantaram discussão sobre os critérios de integração de determinadas instituições no âmbito da aplicação e apresentaram outras sugestões sobre esta matéria.

Opiniões	Concorda		Não concorda		Outras
	Sector	Público	Sector	Público	
N.º	20	96	0	6	47
Percentagem	68,64%		3,55%		27,81%



- **Síntese das opiniões**

Os representantes do sector público consideram que devem regular-se ou emitir-se instruções às situações em que os sistemas informáticos e segurança da rede do órgão ou serviço público sejam assegurados por outro órgão ou serviço público.

Análise e resposta

O gestor do sistema da rede está sujeito à "Lei da Cibersegurança"; quando os sistemas informáticos e a rede de um determinado órgão ou serviço público forem fornecidos, suportados e garantidos por outro órgão ou serviço público, será este, na prática, o responsável pela gestão do sistema e pelos deveres de gestão da cibersegurança. Para clarificar este aspecto, propomos clarificar, no projecto de lei, que, nas situações acima referidas, esses órgãos ou serviço público sejam excluídas do âmbito de aplicação da "Lei da Cibersegurança" as situações acima referidas.

- **Síntese das opiniões**

Há opiniões do público que sugerem estender o âmbito de aplicação a todas as entidades que recebem apoio financeiro do Governo da RAEM.

Análise e resposta

Os destinatários da "Lei da Cibersegurança" são os operadores das infra-estruturas críticas. De acordo com este critério de integração, dado que as actividades desenvolvidas pelas essas entidades não têm necessariamente ligação com o funcionamento das infra-estruturas críticas, não convém estender o âmbito de aplicação a todas as entidades financeiramente apoiadas pelo Governo da RAEM.

Breve conclusão

A maioria das opiniões concorda com o âmbito da aplicação dos "operadores das infra-estruturas críticas". Após a análise das opiniões recolhidas, o Governo vai clarificar normas relativas às exclusões e isenção do âmbito de aplicação no sentido

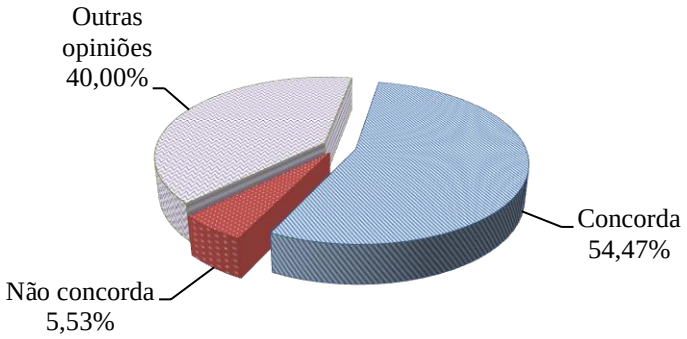
de responder às dúvidas apresentadas pelos sectores e pelo público.

3.2 Os operadores privados das infra-estruturas críticas

Vários serviços públicos importantes tendem actualmente a ser entregues à "exploração privada", sendo que estas entidades privadas e os serviços públicos são considerados, na sociedade moderna, prestadores de serviços públicos; assim, no documento de consulta, propõe-se considerar as entidades privadas, estritamente ligados com as actividades das infra-estruturas críticas, nos 11 domínios nele especificados, como "operadores privados das infra-estruturas críticas".

Relativamente ao âmbito de aplicação dos "operadores privados das infra-estruturas críticas", foram recolhidas 128 opiniões concordantes, 13 opiniões discordantes, tendo recolhidas outras 94 opiniões com entendimentos diferentes dos critérios do âmbito de aplicação; alguns opinantes suscitaram, ainda, a possibilidade de incluir outros determinados sectores nos operadores privados das infra-estruturas críticas.

Opiniões	**Concorda**		**Não concorda**		**Outras**
	Sector	**Público**	**Sector**	**Público**	
N.º	27	101	1	12	94
Percentagem	54,47%		5,53%		40%



■ **Síntese das opiniões**

Relativamente ao âmbito dos operadores privados das infra-estruturas críticas, os representantes dos sectores sugeriram alargá-lo a diversos sectores e associações cívicas, alterando o contexto de "as sociedades de capitais exclusivamente públicos" para "as pessoas colectivas cujo capital seja detido numa percentagem superior a 50%, directa ou indirectamente, pelos serviços públicos"; outras opiniões provenientes do público consideram que devem incluir-se as pequenas e médias empresas *(por exemplo, as companhias*

fornecedoras de gás), as escolas, as clínicas privadas, entre outras entidades que recolhem e conservam uma grande quantidade de dados pessoais.

Análise e resposta

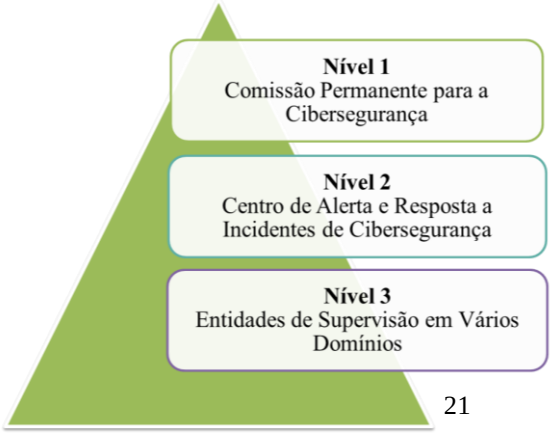
Mesmo que os diversos sectores referidos *(associações cívicas, clínicas, institutos de ensino superior, escolas do ensino primário e secundário ou "pessoas colectivas cujo capital seja detido numa percentagem superior a 50%, directa ou indirectamente, pelos serviços públicos", entre outras entidades)* fossem atingidos por ataques cibernéticos, tal não teria, certamente, impacto seja muito desastroso no funcionamento da sociedade de Macau em geral; por outro lado, a maior parte dessas entidades pode não ter recursos suficientes para cumprir plenamente os deveres estipulados na "Lei da Cibersegurança". Embora essas entidades possam guardar grande quantidade de dados pessoais, tudo isto já está regulado na "Lei da Protecção de Dados Pessoais", pelo que não sugerimos que as mesmas sejam incluídas nas entidades supervisionadas. Além disso, após a entrada em vigor da "Lei da Cibersegurança", o Governo continuará a acompanhar atempadamente a revisão do respectivo âmbito de aplicação.

Breve conclusão

Os sectores e o público concordam, na generalidade, com o âmbito de aplicação dos "operadores privados das infra-estruturas críticas", tendo-se registado 13 opiniões que não concordam com esta matéria, as quais são principalmente provenientes do público, por umas suscitarem preocupações de violação eventual da privacidade pessoal e da liberdade de expressão pela supervisão da cibersegurança, ou outras discordarem directamente a legislação do sistema de protecção da cibersegurança em Macau.

4. Entidades supervisoras do Governo

O documento de consulta propõe um enquadramento funcional de três níveis ao sistema de supervisão da cibersegurança: o nível 1: a "Comissão Permanente para a Cibersegurança", órgão no topo hierárquico; o nível 2: o "Centro de Alerta e Resposta a Incidentes de Cibersegurança", órgão operacional e coordenador: o nível 3: as



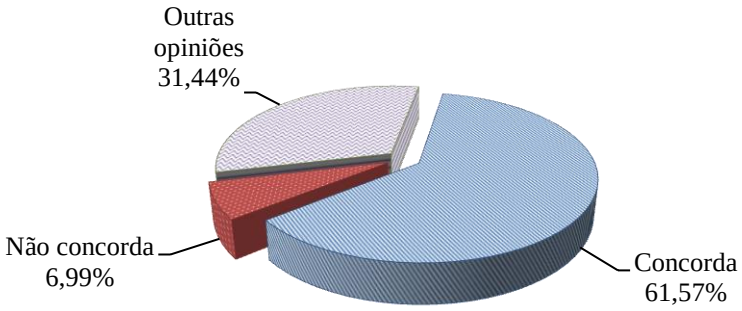
"Entidades de supervisão em vários domínios".

4.1 "Comissão Permanente para a Cibersegurança"

A "Comissão Permanente para a Cibersegurança" é um órgão decisório no topo hierárquico da Cibersegurança, que supervisiona a situação da cibersegurança da RAEM em geral, e ao qual compete principalmente definir o rumo, os objectivos e as estratégias, em geral, da cibersegurança.

No que se refere à "Comissão Permanente para a Cibersegurança", foram recolhidas 141 opiniões concordantes, 16 opiniões discordantes, tendo-se registados outras 72 opiniões que apresentaram sugestões sobre a natureza e a qualidade dos membros da Comissão.

Opiniões	Concorda		Não concorda		Outras
	Sector	Público	Sector	Público	
N.º	17	124	0	16	72
Percentagem	61,57%		6,99%		31,44%



- **Síntese das opiniões**

Os sectores e o público sugerem convidar representantes e especialistas de diferentes áreas para fazer parte dos membros da Comissão, nomeadamente os especialistas da área da cibersegurança, os deputados da Assembleia Legislativa dos sectores informático, representantes das instituições académicas nesta área, juristas, representantes das associações cívicas, entre outros.

Análise e resposta

No âmbito dos regulamentos administrativos complementares da Comissão, será regulado que o presidente da Comissão pode convidar para participar nas

reuniões ou nos trabalhos desenvolvidos pela Comissão, outras entidades públicas ou privadas ou outras individualidades cujo contributo entenda útil aos trabalhos a desenvolver de modo a poder ouvir os pareceres profissionais e técnicas quando a Comissão exercer as suas atribuições na discussão das estratégias e diplomas da cibersegurança.

Breve conclusão

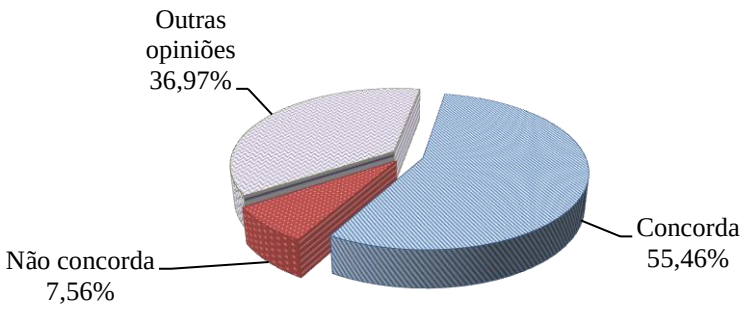
Os sectores e o público concordam, na generalidade, com o estabelecimento e composição da Comissão, tendo-se registado 16 opiniões discordantes provenientes do público, as quais resultam, principalmente, dos entendimentos diferentes quanto à composição dos membros da Comissão ou da discordância com a legislação do estabelecimento do sistema de protecção da cibersegurança em Macau, pelo que não concordam com as disposições propostas nesta matéria.

4.2 "Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC)"

O documento de consulta propõe criar o CARIC como uma organização principal para a concretização do trabalho de prevenção no âmbito da cibersegurança, a quem competirá a monitorização dos dados da rede sob a forma de linguagem máquina, entre os sistemas informáticos 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.

Relativamente à criação e composição do CARIC, foram recolhidas 132 opiniões concordantes, 18 opiniões discordantes; registarem-se 88 opiniões que apresentaram sugestões concretas sobre o funcionamento e as competências do CARIC, bem como sobre a relação dos deveres entre o CARIC, as entidades supervisoras e as entidades supervisionadas.

Opiniões	**Concorda**		**Não concorda**		**Outras**
	Sector	**Público**	**Sector**	**Público**	
N.º	22	110	0	18	88
Percentagem	55,46%		7,56%		36,97%



- **Síntese das opiniões**

As opiniões dos sectores concentram-se na supervisão dos dados da rede *(tais como os critérios da supervisão, métodos concretos, âmbitos e níveis de supervisão)* a efectuar pelo CARIC, assim como o conteúdo sobre a cooperação entre o Centro e as entidades supervisionadas, apresentando várias sugestões concretas e apontando para que as instruções devam ser definidas com clareza.

Análise e resposta

Ao CARIC competirá apenas supervisionar a dimensão do fluxo dos dados da rede e os códigos particulares, com o objectivo de ajudar na descoberta de eventuais dados maliciosos associados aos ataques cibernéticos. Após a publicação oficial da "Lei da Cibersegurança", o Governo vai definir as referidas instruções, em conjunto com os sectores, e providenciar atempadamente orientações técnicos e formação adequada.

- **Síntese das opiniões**

Nas opiniões provenientes dos sectores e do público apresentaram-se sugestões concretas em vários aspectos, nomeadamente quanto ao mecanismo de comunicação dos incidentes da cibersegurança, aos meios de divulgação e recepção das informações da cibersegurança, aos cursos de formação e as acções de sensibilização da cibersegurança. É sugerido, por exemplo, que seja estabelecido um mecanismo de comunicação e cooperação com o exterior no âmbito da cibersegurança, uma linha aberta de 24h, e que sejam organizados simulacros de resposta a incidentes da cibersegurança.

Análise e resposta

Após o estabelecimento do CARIC, o Governo irá, de acordo com as atribuições legais, criar um mecanismo de cooperação em comunicação com o exterior no âmbito da cibersegurança, divulgar e receber, através de diversos meios, as informações importantes relacionadas com a cibersegurança, de modo a melhorar a consciência e aumentar a capacidade da sociedade na protecção da segurança da rede. Além disso, o Governo planeia atender pedidos de esclarecimentos, denúncias e reclamações ligados à cibersegurança, por formulários via electrónica, *e-mails*, entre outros meios, para efeitos do devido acompanhamento. O CARIC irá ainda realizar, periodicamente, simulacros de comunicação e de resposta a incidentes da cibersegurança, reforçando a capacidade de coordenação e reacção dos participantes perante incidentes da cibersegurança.

- **Síntese das opiniões**

Algumas das opiniões oriundas do público manifestam discordância com a supervisão do fluxo de dados e das características dos datagramas, considerando que tal possa prejudicar a privacidade pessoal, a liberdade de expressão, a liberdade de edição ou o segredo comercial.

Análise e resposta

O CARIC vão apenas proceder, durante a supervisão, a uma averiguação da dimensão do fluxo de dados e das características dos datagramas, sem conservar a dimensão do fluxo de dados examinada, nem registar qualquer dado, muito menos decifrar qualquer conteúdo ou discurso que se encontre em rede. Por isso, o pessoal das entidades de supervisão não pode obter quaisquer dados pessoais directamente ou mediante o recurso à técnica de recuperação dos datagramas, informações relativas aos sectores ou conteúdo das comunicações, sob pena de o pessoal responsável pela supervisão assumir as responsabilidades penais e responsabilidades decorrentes da infracção administrativa previstas na Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais), Lei n.º 11/2009 (Lei de combate à criminalidade informática) e Código Penal, bem como as responsabilidades disciplinares previstas no ETAPM. Quando reunidos os pressupostos, poderão assumir responsabilidade civil, em conformidade com o estabelecido no Código Civil.

Para além disso, o sistema jurídico vigente prevê diferentes meios de impugnação administrativa e contenciosa, para garantir a legalidade das actividades administrativas das autoridades; aliás, o documento de consulta da "Lei da Cibersegurança" propõe também estabelecer diferentes níveis de mecanismo de supervisão, no intuito de garantir que as supervisões efectuadas no âmbito da cibersegurança não prejudiquem os dados pessoais, nem ofendam a liberdade de expressão e de edição.

Breve conclusão

As opiniões dos sectores e do público concordam, na generalidade, com o estabelecimento e a composição do CARIC, sendo todas as opiniões discordantes provenientes do público, nas quais se suscitam preocupações de que as actividades de supervisão desenvolvidas pelo CARIC possam causar danos à privacidade pessoal, à liberdade de imprensa, entre outros direitos legítimos.

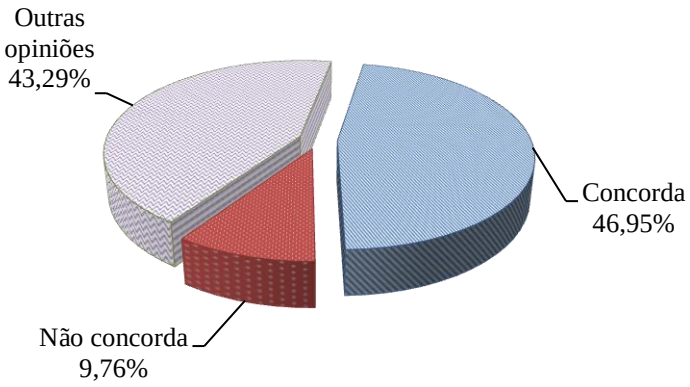
Posto isto, o Governo reforçará as acções de divulgação para dar conhecer à comunidade o modelo de funcionamento do CARIC e que as suas actividades de supervisão não vão afectar a privacidade pessoal ou a liberdade de expressão.

4.3 Entidades supervisoras em vários domínios

De acordo com o documento de consulta, o nível 3 do sistema de supervisão - as **"entidades supervisoras em vários domínios"**, será dividido em duas partes: os órgãos e entidades públicos serão supervisionados pelos SAFP; os operadores das infra-estruturas críticas do sector privado serão supervisionados por 11 serviços públicos relacionados com as áreas de actividade envolvidas ou a natureza desses operadores.

Relativamente à composição das "entidades supervisoras em vários domínios" foram recolhidas 77 opiniões concordantes e 16 opiniões discordantes; registam-se 71 opiniões que suscitaram a questões sobre o âmbito de aplicação das "entidades supervisoras em vários domínios" e a definição da relação da supervisão, entre outros, bem como apresentaram outras sugestões.

Opiniões	**Concorda**		**Não concorda**		**Outras**
	Sector	**Público**	**Sector**	**Público**	
N.º	20	57	0	16	71
Percentagem	46,95%		9,76%		43,29%



- **Síntese das opiniões**

As opiniões dos sectores e do público consideram que a supervisão deve ser implementada por uma única organização enquanto principal entidade de supervisão, e os critérios de gestão da cibersegurança devem ser elaborados de forma uniformizada, para elevar a eficácia de supervisão.

Análise e resposta

A "Lei da Cibersegurança" tem como finalidade a criação de um completo sistema de protecção da cibersegurança, através do qual, a sociedade em geral e os serviços públicos asseguram, em conjunto, a cibersegurança, sendo assim que a cibersegurança dependerá da implementação e execução conjunta pela sociedade, serviços públicos e infra-estruturas críticas, e será mais adequado proceder a supervisão através dos serviços especializados dos respectivos domínios por causa da especificidade de cada tipo das infra-estruturas críticas.

- **Síntese das opiniões**

Há opiniões que manifestam preocupações com que as entidades de supervisão em vários domínios careçam de capacidade técnica suficiente para supervisionar a situação da cibersegurança das entidades supervisionadas.

Análise e resposta

O CARIC vai coordenar a cooperação e acções adequadas entre os diversos intervenientes, prestar instruções técnicas necessárias às entidades de supervisão, de modo a apoiar-lhes a resolver as questões técnicas e assegurar o cumprimento efectivo das suas funções.

- **Síntese das opiniões**

Há opiniões que questionam se as entidades de supervisão irão, invocando o cumprimento dos deveres pelas entidades supervisionadas, exigir a estas últimas a disponibilização de dados de segredo ou informações, o que ofenderá a liberdade de expressão ou liberdade de imprensa.

Análise e resposta

O pessoal das entidades supervisoras apenas poderá entrar nas instalações dos operadores das infra-estruturas críticas para conhecer a realidade, quando as suas redes sofrerem ataques ou invasões. Mesmo que o pessoal da entidade supervisora exija o acesso dos dados durante a inspecção, não lhe é permitido obter os dados operacionais da actividade dos operadores das infra-estruturas críticas, nem os dados pessoais dos clientes, entre outras informações confidenciais; os dados pessoais e conteúdos de comunicação não poderão ser consultados ou obtidos pelo pessoal de supervisão, salvo o consentimento expresso das entidades supervisionadas ou a autorização pelo juiz devido à necessidade da investigação criminal de acordo com as disposições do Código de Processo Penal, caso contrário o pessoal de supervisão assumirá as responsabilidades penais e responsabilidades decorrentes da infracção administrativa previstas na Lei n.º 8/2005 (Lei da Protecção de Dados Pessoais), Lei n.º 11/2009 (Lei de combate à criminalidade informática) e Código Penal, bem como as responsabilidades disciplinares previstas no ETAPM e a eventual responsabilidade civil.

Para além de definir as políticas de cibersegurança de Macau, cabe à "Comissão Permanente para a Cibersegurança" a supervisão do funcionamento regular da estrutura de supervisão da cibersegurança, nomeadamente a supervisão do trabalho desenvolvido pelo CARIC e pelas entidades de supervisão em diversos domínios. Se os operadores das infra-estruturas críticas sujeitos à supervisão ou quaisquer indivíduos suspeitarem que a entidade de supervisão da cibersegurança age ilegalmente ou de uma forma injusta no exercício do poder público, poderão recorrer aos meios de impugnação previstos na lei. A "Lei da Cibersegurança" definirá uma série de mecanismos de supervisão de diversos níveis, que visam a garantir que as actividades de supervisão da cibersegurança não causem danos aos dados pessoais, nem ofendam a liberdade de expressão e a liberdade de imprensa.

Breve conclusão

As opiniões dos sectores mostram-se concordantes com o estabelecimento das "entidades de supervisão em vários domínios", ao passo que as opiniões discordantes são provenientes de alguns cidadãos, por duvidarem a capacidade das técnicas de supervisão da cibersegurança das entidades de supervisão e estarem preocupados com que a supervisão da cibersegurança efectuada pelas entidades de supervisão possa prejudicar a liberdade de expressão ou de imprensa.

5. Deveres legais

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

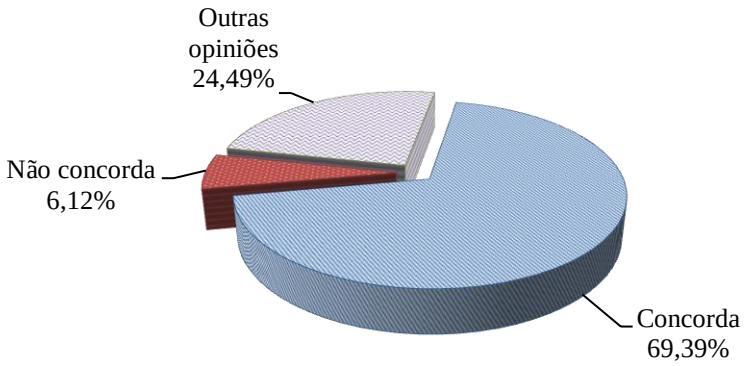
5.1 Deveres de carácter orgânico

O documento de consulta propõe que os operadores privados das infra-estruturas críticas devem criar unidades especializadas de gestão da cibersegurança e designar responsável, proceder à verificação de idoneidade e de antecedentes na experiência profissional do responsável e dos técnicos em lugares-chave, e estabelecer mecanismos e meios para apresentar reclamações e denúncias relacionadas com a cibersegurança.

Relativamente aos "deveres de carácter orgânico" foram recolhidas 68 opiniões concordantes, 6 discordantes com a criação de unidade da cibersegurança e designação do responsável; 56 opiniões concordantes e 7 discordantes com a verificação de antecedentes do responsável de cibersegurança e dos técnicos em lugares-chave. Por outro lado, 45 opiniões apresentaram sugestões sobre o procedimento de verificação da idoneidade, as responsabilidades e dos antecedentes do responsável de cibersegurança.

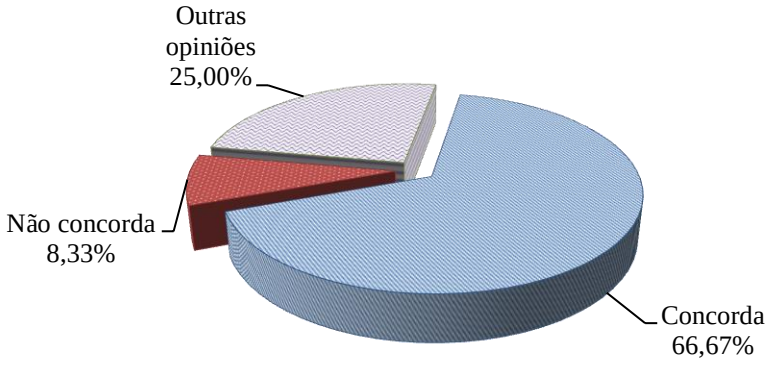
Criação da unidade especializada na gestão da cibersegurança e designação do respectivo responsável

Opiniões	Concorda		Não concorda		Outras
	Sector	Público	Sector	Público	
N.º	38	30	1	5	24
Percentagem	69,39%		6,12%		24,49%



Verificação de antecedentes de responsável da cibersegurança e técnicos em lugares-chave

Opiniões	Concorda		Não concorda		Outras
	Sector	Público	Sector	Público	
N.º	31	25	1	6	21
Percentagem	66,67%		8,33%		25%



- **Síntese das opiniões**

Os sectores levantaram questões sobre a idoneidade para assumir o cargo, a experiência profissional, a identidade e o domicílio do responsável da cibersegurança, bem como a possibilidade de "*outsourcing*".

Análise e resposta

O principal papel do responsável da cibersegurança é administrador e não operador, pelo que nem sempre necessitará de ser assumido por pessoa com conhecimentos profissionais na área da cibersegurança; o Governo não definiu requisitos específicos quanto à experiência profissional do responsável da cibersegurança, exigindo apenas a intervenção da PJ na verificação dos seus antecedentes criminais.

No documento de consulta não está definido se o cargo de responsável da cibersegurança precisa de ser assumido por um residente ou não-residente de Macau. Para garantir a comunicação e o papel intermédio do responsável, o projecto de lei preverá que o principal responsável de cibersegurança deve ter residência habitual na RAEM, estar permanentemente contactável pelo CARIC e assegurar que, nas suas faltas ou impedimentos, está disponível na RAEM e igualmente contactável um outro interlocutor habilitado, conhecedor dos sistemas. Caso seja nomeado um responsável não-residente de Macau para o cargo de responsável da cibersegurança, este só poderá ser recrutado nos termos da lei de Macau e em conformidade com as disposições dos diplomas sobre o regime de permanência e de migração, necessitando de apresentar as respectivas informações do registo criminal do exterior para que o Governo proceda os trabalhos de verificação.

Além disso, para se tornar mais clara a delegação de trabalho da cibersegurança a entidades terceiras, foram acrescentadas algumas disposições no projecto de lei, onde é explicitado que os operadores das infra-estruturas críticas não devem, sob o pretexto da delegação a entidades terceiras, tentar desviar e eximir-se da obediência aos deveres e das responsabilidades para evitar quaisquer contornos da lei e fuga à responsabilidade.

- **Síntese das opiniões**

Relativamente à exigência da idoneidade no aspecto de verificação de antecedentes constante no documento de consulta, um cidadão sugeriu a proibição de contratação para o referido cargo de pessoa que tenha sido condenada por quaisquer factos criminosos *(independentemente do prazo da pena de prisão)* por decisão transitada em julgado.

Análise e resposta

O documento de consulta sugere que a pessoa com certos registos criminais não pode assumir o cargo de responsável da cibersegurança, disposição que visa impedir aqueles que tenham praticado condutas criminosas directamente relacionadas com os requisitos do referido cargo ou aqueles que tenham praticado crimes graves, a assumir o cargo; quanto às pessoas com outro tipo de registos criminais, cabe aos operadores decidir se é apropriado contratá-las para o referido cargo.

- **Síntese das opiniões**

Nas opiniões dos sectores, pretende-se conhecer o "mecanismo e meios para apresentar reclamações e denúncias relacionadas com a cibersegurança" referido no documento de consulta, questionando-se se o mesmo deve funcionar 24 horas por dia, se todas as reclamações e denúncias dos incidentes deverão ser comunicadas para registo e a qual entidade devem ser comunicadas.

Análise e resposta

Após a publicação da "Lei da Cibersegurança", o Governo irá definir, junto dos sectores, com mais clareza, através de instruções, os requisitos sobre os deveres dos operadores privados sobre o estabelecimento do "mecanismo e meios para apresentar reclamações e denúncias relacionadas com a cibersegurança".

- **Síntese das opiniões**

Houve opinantes que se preocuparam em saber se, ocorrendo incidentes de cibersegurança, o respectivo responsável terá de assumir toda a responsabilidade da instituição.

Análise e resposta

Os destinatários da "Lei da Cibersegurança" são os operadores das infra-estruturas críticas e as responsabilidades resultantes do incumprimento ou infracção dos deveres da cibersegurança serão assumidas pela respectiva instituição; mesmo que a instituição considere que essa violação foi causada pela negligência de um funcionário, as responsabilidades legais ficarão sempre a cargo da mesma.

Breve conclusão

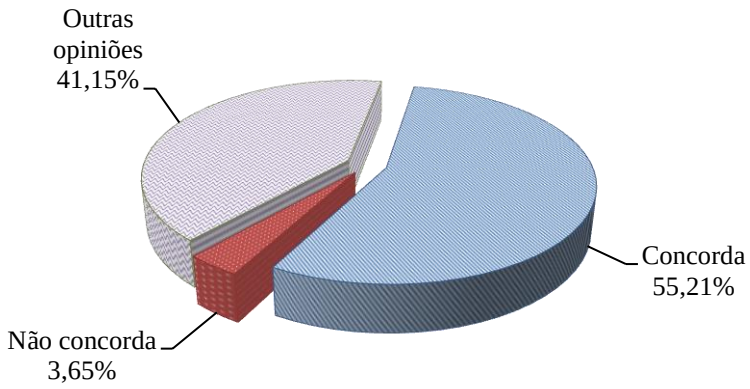
As opiniões dos sectores e do público em geral manifestam-se de acordo com a criação de unidades da cibersegurança e designação do respectivo responsável, e a verificação de antecedentes de técnicos em lugares-chave. A esse respeito, as opiniões discordantes são, principalmente, provenientes do público, por divergirem com o constante no documento da consulta relativo à verificação de registo criminal, ou não concordarem com a legislação sobre a criação do sistema de protecção da cibersegurança.

5.2 Deveres de carácter procedimental, preventivo e reactivo

O documento de consulta sugere que os operadores das infra-estruturas críticas devem estabelecer um regime de gestão da cibersegurança e procedimentos operacionais, implementar medidas internas de protecção, monitorização, alerta e resposta às emergências da cibersegurança e informar o Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC) da ocorrência de tais incidentes, dando conhecimento do facto à respectiva entidade.

No que diz respeito aos deveres de carácter procedimental, preventivo e reactivo", registam-se 106 opiniões concordantes e 7 discordantes e 79 outras opiniões em que se discute ou opina sobre as questões do funcionamento prático e a elaboração de instruções concretas no futuro.

Opiniões	**Concorda**		**Não concorda**		**Outras**
	Sector	**Público**	**Sector**	**Público**	
N.º	35	71	1	6	79
Percentagem	55,21%		3,65%		41,15%



- **Síntese das opiniões**

De modo geral, os sectores preocupam-se com a disponibilização ou não, pelas entidades supervisoras, de instruções com critérios concretos e uniformizados acerca do regime de gestão e procedimento de funcionamento às entidades supervisionadas, sugerindo ao Governo definir minuciosamente o estabelecimento de regime de níveis para os incidentes da cibersegurança, o mecanismo de comunicação e os critérios de comunicação.

Análise e resposta

O "Centro de Alerta e Resposta a Incidentes de Cibersegurança" definirá, de acordo com a prática internacional, graus para incidentes de cibersegurança, enquanto a "Comissão Permanente para a Cibersegurança", o próprio "Centro de Alerta" e as entidades supervisoras de diversos sectores cooperarão com os operadores das infra-estruturas críticas das respectivas áreas, estabelecendo um regime de gestão da cibersegurança, procedimentos operacionais e padrões concretos adequados aos respectivos sectores conforme as suas situações reais, entre os quais se incluirão as instruções da gestão hierárquica acerca da cibersegurança e a sua comunicação.

- **Síntese das opiniões**

Tanto os diversos sectores como o público acham que os operadores das infra-estruturas críticas devem proceder, periodicamente, a testes e actualizações de resposta a emergências.

Análise e resposta

A "Comissão Permanente para a Cibersegurança", o "Centro de Alerta e Resposta a Incidentes de Cibersegurança" e as entidades supervisoras dos diversos sectores organizarão periodicamente simulacros relativos a incidentes de cibersegurança, juntamente com os operadores de infra-estruturas críticas, no sentido de intensificar a capacidade de colaboração e elevar o nível técnico das entidades participantes na resposta à emergência.

Breve conclusão

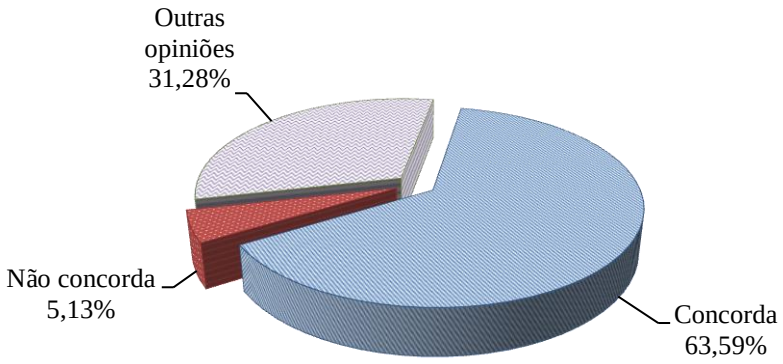
Os diversos sectores e o público concordam, em geral, quanto aos deveres de carácter procedimental, preventivo e reactivo do documento de consulta; as opiniões discordantes são principalmente do público, por considerarem que a protecção da cibersegurança é dever das instituições públicas e privadas, devendo estas, por sua iniciativa, estabelecer procedimentos ou medidas relacionadas com a protecção da sua cibersegurança, e não sendo, de modo algum, necessária a criação da "Lei da Cibersegurança" para a respectiva regulamentação.

5.3 Deveres de auto-avaliação e relato

No documento da consulta propõe-se que os operadores das infra-estruturas críticas procedem, com o próprio pessoal ou com a intervenção de entidades profissionais a quem deleguem, a avaliação da segurança e dos eventuais riscos existentes nas suas redes, submetendo à respectiva entidade de supervisão um relatório sobre a cibersegurança.

Quanto ao que se refere aos "deveres de auto-avaliação e relato", registam-se 124 opiniões concordantes e 10 discordantes; foram recolhidas 61 opiniões que suscitaram questões sobre os critérios para efeitos da avaliação e as instituições profissionais que se responsabilizam pela avaliação dos riscos da cibersegurança.

Opiniões	Concorda		Não concorda		Outras
	Sector	Público	Sector	Público	
N.º	46	78	3	7	61
Percentagem	63,59%		5,13%		31,28%



- **Síntese das opiniões**

As opiniões e sugestões dos sectores reportam-se principalmente ao critério de verificação, o âmbito de verificação, a forma e a frequência de avaliação, bem como o modelo de relatório a submeter e o seu conteúdo, entre outros.

Análise e resposta

A "Comissão Permanente para a Cibersegurança", "o Centro de Alerta e Resposta a Incidentes de Cibersegurança" e as entidades supervisoras dos diversos domínios definirão uma série de orientações adequadas aos sectores em causa, nomeadamente no que diz respeito ao âmbito da avaliação, aos critérios e modos a usar, aos modelos e ao teor do relatório, tendo em conta a dimensão das infra-estruturas críticas e sua capacidade de contrair encargos. Para além disso, as entidades supervisoras analisarão e avaliarão o relatório da segurança da rede e, em caso necessário, poderão solicitar ao Centro de Alerta e Resposta a Incidentes de Cibersegurança a emissão de pareceres técnicos. Após a publicação da Lei da Cibersegurança, o prazo de entrega do relatório, as medidas de salvaguarda do sigilo, além dos outros assuntos específicos, serão regulados através de instruções ou documentos normativos.

- **Síntese das opiniões**

Algumas opiniões dos sectores e do público indicaram que em alguns países e regiões se impõe avaliação de segurança da rede por terceiros, sugerindo que Macau pode tomar como referência.

Análise e resposta

Propõe-se, no documento de consulta, que os operadores das infra-estruturas críticas devam proceder, com o próprio pessoal ou com a intervenção de entidades profissionais que deleguem, a avaliação da segurança e dos eventuais riscos existentes na rede, uma vez que, por razões de confidencialidade ou de segurança, alguns serviços públicos não têm condições de permitir a terceiros fazer a respectiva avaliação. Assim, chega-se à conclusão de que as entidades supervisionadas devem tomar a decisão consoante a própria situação real.

Breve conclusão

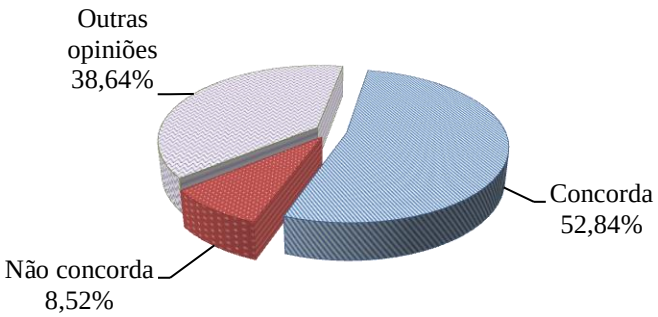
A maioria das opiniões dos sectores e do público manifesta-se concordante no que diz respeito aos "deveres de auto-avaliação e relato", tendo-se sugerido o aperfeiçoamento quanto à avaliação concreta e ao conteúdo do relatório em causa. Por conseguinte, as autoridades ponderá-lo-ão no acto de aperfeiçoamento do conteúdo do projecto de lei.

5.4 Dever de colaboração

É proposto no documento de consulta que, na medida necessária do cumprimento dos deveres de carácter procedimental, preventivo e reactivo, os operadores das infra-estruturas críticas permitem a entrada do pessoal do Centro de Alerta e Resposta a Incidentes de Cibersegurança ou das entidades de supervisão nas suas instalações, e disponibilizar-lhes as informações para a sua verificação.

Relativamente ao "dever de colaboração" foram recolhidas 93 opiniões concordantes e 15 discordantes; outras 68 opiniões referem-se ao procedimento, ao tempo de estadia e pedido de informações na entrada das instalações das infra-estruturas críticas do pessoal supervisionado.

Opiniões	Concorda		Não concorda		Outras
	Sector	Pública	Sector	Público	
N.º	27	66	1	14	68
Percentagem	52,84%		8,52%		38,64%



- **Síntese das opiniões**

As opiniões dos sectores reportam-se principalmente ao âmbito de aplicação, à competência e aos tipos de informações acessíveis, etc., do CARIC ou do pessoal das entidades supervisora no exercício das funções.

Análise e resposta

Só quando houver certos sinais indicando que as entidades supervisionadas não cumprem os deveres estipulados na Lei da Cibersegurança, ou quando ocorreu ou é possível ter ocorrido um incidente de cibersegurança nas entidades supervisionadas, o CARIC e as entidades de supervisão podem enviar pessoal ao local de trabalho dos operadores das infra-estruturas críticas para verificar o procedimento de segurança da rede e o cumprimento dos deveres, ou recolher provas relativas ao ataque cibernético; o Governo comunicará previamente, às entidades supervisionadas envolvidas, com a maior brevidade possível, o envio de pessoal para a finalidade referida.

Além disso, o Governo procederá às alterações no conteúdo da proposta relativamente aos "deveres de procedimento, preventivo e reactivo", prevendo expressamente que apenas terá lugar a entrada do pessoal das entidades de supervisão nas instalações dos operadores privados das infra-estruturas críticas para apurar a veracidade dos factos quando houver invasão ou ataques nas suas redes, ou acontecerem outras acções não autorizadas.

- **Síntese das opiniões**

Houve cidadãos e órgãos de comunicação social que sugeriram prever-se expressamente no projecto de lei quais as informações cuja disponibilização será solicitada aos operadores das infra-estruturas críticas, de forma a evitar o abuso das disposições que eventualmente podem servir como ferramenta para violar a privacidade pessoal, o sigilo das comunicação e a liberdade de imprensa.

Análise e resposta

Ao cumprir os "deveres de colaboração", o responsável da cibersegurança do operador das infra-estruturas críticas pode manter-se no local para participar no procedimento de supervisão realizada pelo pessoal do CARIC e das entidades de supervisão, de modo de garantir o seu justo acesso dos dados, com a excepção dos dados confidenciais, nomeadamente dados de negociações e dados pessoais dos clientes das entidades supervisionadas. Por outro lado, os dados pessoais e conteúdos de comunicação não podem ser consultados ou acedidos pelo pessoal de supervisão, salvo nos casos em que as entidades supervisionadas possam dar o seu consentimento expresso ou mediante autorização pelo magistrado, devido à necessidade da investigação criminal de acordo com as disposições do Código de Processo Penal.

Breve conclusão

Na maioria absoluta das opiniões dos sectores, verificou-se concordância com o "dever de colaboração"; as opiniões discordantes provêem, principalmente, do público, invocando-se a possibilidade de se obter os dados pessoais dos cidadãos sob pressuposto do "dever de colaboração" ou ter-se acesso directo, a qualquer tempo, às instituições de comunicação social e exigir-se disponibilização das informações pretendidas, facto este que possibilitará prejudicar a liberdade de imprensa, até interferir nos dados informáticos lançados em comunicações de imprensa.

Pelo exposto, após a entrada em vigor da lei, o Governo irá, por diversas vias, reforçar actividades de sensibilização e divulgação, de forma a esclarecer as dúvidas dos cidadãos e, ao mesmo tempo, clarificar a regulamentação do trabalho do CARIC e das entidades de supervisão.

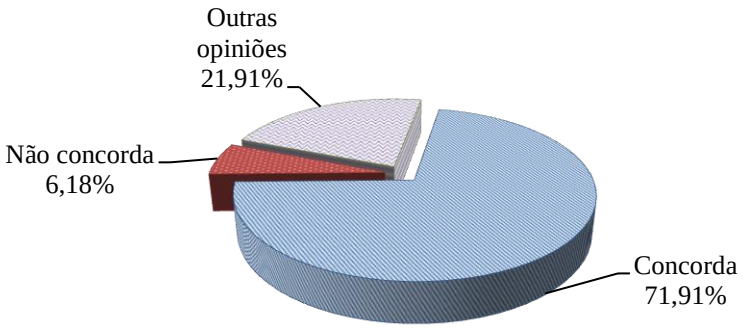
5.5 Deveres especiais dos operadores da rede pública

Para além dos "deveres de carácter orgânico", "deveres de carácter procedimental, preventivo, reactivo", "deveres de auto-avaliação" e "deveres de colaboração", propõe-se ainda, no documento de consulta, que os operadores da rede pública também devem cumprir mais dois deveres, designadamente o dever de implementar o "*Real-Name System*" e de proceder à conservação de registos "*Web-logs*".

Foram recolhidas dos sectores e do público, 128 opiniões concordantes e 11 discordantes com a implementação do "*Real-Name System*", bem como 35 opiniões concordantes e 8 discordantes com a conservação de registos "*Web-logs*". Além disso, registam-se 52 opiniões que se referem a outras matérias relacionadas, tais como a forma de registo do "*Real-Name System*", o prazo da conservação de registos "*Web-logs*" e a protecção dos dados pessoais.

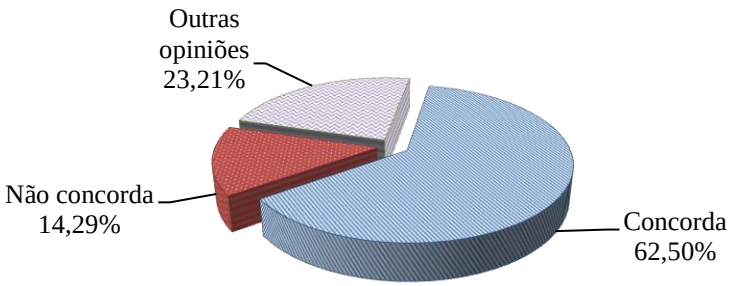
"*Real-Name System*"

Opiniões	Concorda		Não concorda		Outras
	Sector	**Público**	**Sector**	**Público**	
N.º	21	107	0	11	39
Percentagem	71,91%		6,18%		21,91%



Conservação de registos "*Web-logs*"

Opiniões	Concorda		Não concorda		Outras
	Sector	**Público**	**Sector**	**Público**	
No.	16	19	0	8	13
Percentagem	62,5%		14,29%		23,21%



- **Síntese das opiniões**

As opiniões e sugestões provenientes dos diversos sectores concentram-se essencialmente no âmbito de aplicação dos deveres do "*Real-Name System*", na concretização da sua implementação e na protecção aos dados pessoais individuais, propondo-se também que as entidades supervisoras providenciem orientações técnicas e das responsabilidades em detalhe, mas precedidas de troca de ideias com os operadores.

Análise e resposta

Segundo a prática comum a nível internacional, após a implementação do "*Real-Name System*", os utentes de telemóveis serão obrigados a fornecer os dados de identificação verdadeiros para efeitos de registo ao adquirirem os serviços dos operadores de telecomunicações. De acordo com a situação actual do sector de telecomunicações em Macau, excepto quanto aos cartões pré-pagos, os utentes dos serviços telefónicos fixos e móveis têm de fazer registo com a prestação dos dados de identificação verdadeiros. O "*Real-Name System*" visa impor às pessoas que adquirem cartões pré-pagos que disponibilizem esses dados para efeitos do registo, prevenido que os criminosos utilizem esses cartões não nominais como instrumento para escapar à investigação criminal, de forma a melhor salvaguardar a ordem pública e garantir os direitos e interesses legítimos dos cidadãos em geral. Por conseguinte, a solicitação aos utentes de cartões pré-pagos dos dados é uma exigência básica e, aliás, uma regra comum nos negócios jurídicos. Noutros países, esta regra para proteger o interesse social já foi implementada.

A par disso, os deveres do "*Real-Name System*" também são aplicáveis a entidades que prestem ao público os serviços de acesso à *internet*, incluindo entidades que forneçam serviços públicos de acesso à *internet* sem fios (ex.: *WiFi-Go*). O Governo irá, por diversas vias, promover discussão com os operadores da rede pública sobre a regulamentação para implementar esse sistema e medidas técnicas a nível da sua aplicação.

- **Síntese das opiniões**

Em relação ao "*Real-Name System*", as opiniões dos sectores e do público propõem que os operadores de rede pública introduzam alguns equipamentos e medidas para efectuar registo de forma conveniente e aproveitem ao máximo

meios electrónicos para efectuar registo com vista a minimizar os seus impactos à população.

Análise e resposta

No processo de implementação do "*Real-Name System*", o Governo terá em consideração vários factores, nomeadamente a protecção dos dados pessoais, verificação e actualização de dados de identificação, formalidades convenientes e influências sobre os pequenos retalhistas de telecomunicações, com vista a que o sistema de "*Real-Name System*" seja adequadamente implementado. Além disso, o Governo irá executar as medidas de uma forma faseada, efectuando melhor comunicação e coordenação com os operadores, bem como esforçando-se na procura das medidas que não afectem o funcionamento actual do mercado.

A fim de optimizar as disposições do "*Real-Name System*", o projecto de lei inclui disposições transitórias adequadas, estipulando-se que o utente que tiver comprado um cartão pré-pago antes da entrada em vigor da lei, deverá apresentar os seus dados de identificação verdadeiros dentro de um período determinado após a entrada em vigor da lei, sob a pena de o cartão ser desactivado.

- **Síntese das opiniões**

Verificaram-se algumas opiniões do público não concordantes com os deveres da "Conservação de registos de *Web logs*", por entenderem que as respectivas disposições poderão levar a violação da privacidade pessoal, das comunicações por redes e da liberdade de expressão.

Análise e resposta

A "Conservação de registos de *Web logs*" proposta no documento de consulta, consiste em proceder à conservação dos registos de *Web logs* das translações entre os endereços IP *internet* e os endereços das redes internas dos utilizadores; não se incluem nesses registos, os conteúdos que se referem aos comportamentos praticados por via electrónica ou os registos de páginas visitadas pelos utilizadores. A conservação destina-se a rastrear a identidade verdadeira dos utentes dos endereços IP *internet* envolvidos em crime da rede informática em causa, facilitando assim a investigação do crime. Posto isto, o Governo tenciona substituir a designação da "conservação dos registos de *Web logs*" por "conservação e prestação dos registos de translação de endereços electrónicos",

sugerindo o aditamento de um artigo na Lei n.º 11/2009 (Lei de combate à criminalidade informática) para regular a "conservação dos registos de *Web logs*"; deste modo fica bem explícito que os órgãos de polícia criminal só podem obter, junto dos operadores dos serviços de rede, os "registos de *Web logs*" que conservam após a autorização do juiz, nos termos do regime jurídico do processo penal.

Breve conclusão

Considera-se, em generalidade, nas opiniões dos sectores e do público, que tanto o "*Real-Name System*" como a "conservação dos registos de *Web logs*" podem contribuir para o combate às fontes do crime cibernético e a investigação criminal, reforçando a protecção dos cidadãos.

Foram recolhidas 19 opiniões, todas provenientes do público, que não concordam com a implementação aos deveres do "*Real-Name System*" e da "conservação dos registos de *Web logs*". Não obstante, essa discordância foi originada meramente pela não-compreensão sobre os objectivos da implementação dos dois deveres.

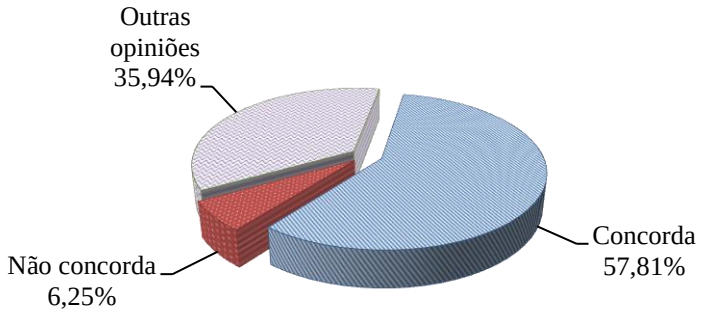
Pelo exposto, o Governo propõe que se proceda a uma alteração ao projecto da lei, substituindo a designação da "conservação dos registos de *Web logs*" por "conservação e prestação dos registos de translação de endereços electrónicos", com vista a que o público fique bem esclarecido de que não se inclui nesses registos os comportamentos praticados por via electrónica ou os registos de páginas visitadas pelos utilizadores.

5.6 Deveres dos operadores públicos das infra-estruturas críticas

Os operadores públicos e privados das infra-estruturas críticas têm de cumprir também os "deveres de carácter procedimental, preventivo, reactivo", os "deveres de auto-avaliação" e os "deveres de colaboração"; mas, quanto aos "deveres de carácter orgânico", apenas se estipula que devem designar, de entre o pessoal da direcção ou equiparado dos operadores públicos das infra-estruturas críticas, uma pessoa para assumir as funções de responsável pela cibersegurança.

Foram recolhidas 37 opiniões concordantes e 4 discordantes com isso; em 23 opiniões, foram apresentadas sugestões sobre o estabelecimento das medidas de protecção de cibersegurança dos serviços públicos.

Opiniões	Concorda		Não concorda		Outras
	Sector	**Público**	**Sector**	**Público**	**Outras**
N.º	18	19	0	4	23
Percentagem	57,81%		6,25%		35,94%



- **Síntese das opiniões**

Nas opiniões dos sectores referiu-se que, actualmente, alguns serviços públicos contratam através de adjudicação empresas/instituições privadas para ajudar a prestar os serviços da rede, sugerindo-se que, no projecto da lei, se definam claramente se os serviços públicos podem, através de adjudicação, contratar empresas/instituições privadas para efectuar a avaliação da cibersegurança.

Análise e resposta

A Comissão Permanente para a Cibersegurança e o CARIC procederão a estudos sobre a implementação dum regime de gestão, do fluxo das operações e dos critérios no âmbito de cibersegurança apropriados aos serviços da Administração de Macau. A par disso, elaborará disposições mais claras sobre a matéria de adjudicação dos serviços da cibersegurança a empresas/instituições privadas.

Breve conclusão

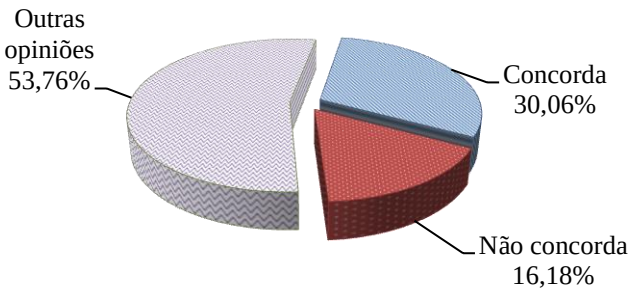
As opiniões dos sectores e do público concordam, em generalidade, com o cumprimento dos deveres dos operadores das infra-estruturas críticas, propostos no documento de consulta.

6. Sanções administrativas e responsabilidades disciplinares pelo incumprimento dos deveres

É proposto no documento de consulta, 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. Àqueles que violem gravemente os deveres, poderão ser aplicadas separada ou cumulativamente sanções acessórias. Relativamente aos operadores públicos das infra-estruturas críticas, os funcionários responsáveis pelo incumprimento dos deveres de cibersegurança, a título de dolo ou negligência, serão sujeitos a responsabilidade disciplinar.

Foram recolhidas, em total, 52 opiniões que concordam e 28 que não concordam com isso, bem como 93 outras opiniões expressando o desejo de que o Governo elabore definições claras sobre infracções leves e graves e aplique outros tipos de sanções para o incumprimento dos deveres, designadamente a submissão às medidas de educação obrigatória ou assunção da responsabilidade penal.

Opiniões	Concorda		Não concorda		Outras
	Sector	**Público**	**Sector**	**Público**	**Outras**
N.º	12	40	4	24	93
Percentagem	30,06%		16,18%		53,76%



- **Síntese das opiniões**

As opiniões dos sectores referem-se à necessidade de elaborar definições claras sobre os níveis de gravidade de infracções e as respectivas sanções pelo incumprimento dos deveres, bem como a introdução do regime de reincidência.

Análise e resposta

As infracções administrativas estipuladas na "Lei da Cibersegurança", para além de serem reguladas pela mesma, são também reguladas pelo regime geral das infracções administrativas, ou seja, o Decreto-Lei n.º 52/99/M, de 4 de Outubro. Quanto à questão das sanções apropriadas relativas às infracções administrativas, são aplicadas, com as necessárias adaptações, as disposições do n.º 2 do artigo 65.º (Determinação da medida da pena) do Código Penal, e o Governo, atendendo a todas as circunstâncias do infractor, avaliando globalmente todos os elementos objectivos, em observação dos princípios estipulados no Código do Procedimento Administrativo, designadamente o princípio de legalidade, o princípio da proporcionalidade, o princípio da boa-fé, princípio da imparcialidade, irá, dentro das espécies e molduras legais, determinar a multa e sanções acessórias adequadas. As entidades supervisionadas podem, por sua parte, impugnar a decisão por via administrativa nos termos do Código do Procedimento Administrativo e por via contenciosa nos termos do Código do Procedimento Administrativo Contencioso. O Governo irá também introduzir, no projecto de lei, disposições relacionadas com a reincidência, por forma a definir explicitamente o conceito e a respectiva agravação.

- **Síntese das opiniões**

Nas opiniões dos sectores, propôs-se que sejam definidos claramente os deveres e as respectivas sanções dos operadores das redes públicas pelo incumprimento do regime da identificação real ("*Real-Name System*") da "conservação dos registos de *Web logs*".

Análise e resposta

Para se articularem estreitamente o conteúdo do "*Real-Name System*" e a "conservação dos registos de *Web logs*" com o regime jurídico dos serviços de *internet*, o Governo irá proceder a ajustamentos e revisão necessários ao projecto da lei, através dos quais se pretende aplicar aos operadores pelo incumprimento dos respectivos deveres a multa mais pesada prevista no Regulamento Administrativo n.º 24/2002 vigente (que estabelece o Regime de Acesso e Exercício da actividade de Prestação de Serviços *Internet*).

■ **Síntese das opiniões**

Verificam-se opiniões do público que sugerem a aplicação das sanções penais às violações graves dos deveres legais.

Análise e resposta

Dado que o regime de cibersegurança é, na sua natureza, um sistema de gestão preventivo, as infracções às disposições preventivas, geralmente, não são criminalizadas. Esta solução é compatível com o "princípio de intervenção mínima do Direito Penal" que caracteriza o sistema jurídico da RAEM. Por esses motivos, não é adequado criminalizar as responsáveis no âmbito de cibersegurança, sem prejuízo da efectivação das responsabilidades penais previstas na demais legislação ou regulamentação.

Breve conclusão

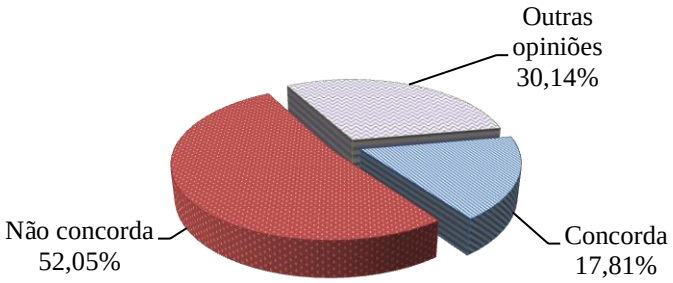
As opiniões dos sectores concordam, na generalidade, com o conteúdo proposto no documento de consulta relativo às "Sanções administrativas e responsabilidades disciplinares pelo incumprimento dos deveres", mas regista-se uma percentagem considerável das opiniões do público que julga que as sanções propostas no documento de consulta são demasiadamente leves.

7. Ponderações especiais sobre a data da entrada em vigor

Propõe-se no documento de consulta que a Lei da Cibersegurança entre em vigor 30 dias após a sua publicação, ressalvando-se, porém, que as datas de entrada em vigor dos 2 deveres especiais da identificação real ("*Real-Name System*") e da "conservação dos registos de *Web logs*" serão previstas posteriormente.

Foram recolhidas 26 opiniões concordantes e 76 discordantes com isso. As opiniões dos diversos sectores consideram, na generalidade, que é necessário mais tempo para a implementação das medidas de cibersegurança; registam-se também 44 opiniões que julgam que o Governo pode proporcionar adequadamente um período transitório aos sectores e sugerem realizar mais actividades de divulgação antes da entrada em vigor da lei.

Opiniões	Concorda		Não concorda		Outras
	Sector	**Público**	**Sector**	**Público**	**Outras**
N.º	9	17	20	56	44
Percentagem	17,81%		52,05%		30,14%



- **Síntese das opiniões**

Em relação à data de entrada em vigor da lei, as opiniões dos sectores consideram, na generalidade, que o período da vacância é demasiado curto, sendo necessário mais tempo para a implementação das respectivas medidas de cibersegurança, tais como a elaboração das soluções, o recrutamento de profissionais, a formação de pessoal e a aquisição de equipamentos.

Análise e resposta

Considerando que os operadores das infra-estruturas críticas necessitam de fazer os preparativos e de se adaptar ao regime de cibersegurança, o Governo irá proceder aos devidos ajustamentos ao período da vacância previsto na lei, de forma a proporcionar condições aos sectores em causa para fazer trabalhos preparativos necessários à implementação da lei.

- **Síntese das opiniões**

As opiniões dos sectores exprimem que é necessário proporcionar-lhes certo tempo para implementar o processo de reconhecimento do regime da identificação real ("*Real-Name System*") e da conservação dos registos das translações entre os endereços da *internet* e de *intranet*, sugerindo que se realize uma abordagem mais pormenorizada sobre essa matéria entre o Governo e os operadores de comunicações.

Análise e resposta

No documento de consulta não está especificada a data de entrada em vigor relativa aos deveres de implementação do "*Real-Name System"* e da conservação de *Web logs*, pois a Administração deseja que a respectiva data fique a ser determinada após discutido com o órgão legislativo e obtido o consenso público, de modo a minimizar o impacto no funcionamento dos sectores e na vida da população.

Breve conclusão

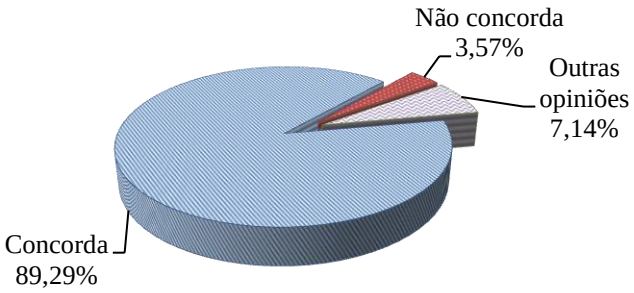
Tendo em conta que a maioria das opiniões dos sectores e do público não concordam com a data da entrada em vigor da Lei da Cibersegurança (30 dias após a sua publicação) e julgam que o período da vacância é demasiado curto, o Governo da RAEM, após a devida consideração, pretende a prolongar o período para a entrada em vigor da Lei, propondo, assim, que a Lei da Cibersegurança entre em vigor 180 dias após a sua publicação, a fim de proporcionar condições aos operadores das infra-estruturas críticas a fazer os respectivos preparativos ao regime da cibersegurança.

8. Regulamentação

O documento de consulta refere que serão regulados pelo regulamento administrativo complementar as atribuições e o funcionamento da "Comissão Permanente para a Cibersegurança" e do "Centro de Alerta e Resposta a Incidentes de Cibersegurança", bem como a designação das entidades públicas responsáveis pela supervisão.

Foram recolhidas 25 opiniões concordantes e 1 discordante com isso, verificando-se também 2 opiniões que sugerem ao Governo que efectue, antes de elaborar a regulamentação, análise profunda sobre as dificuldades técnicas que os diversos sectores poderão encontrar na implementação da Lei da Cibersegurança.

Opiniões	Concorda		Não concorda		Outras
	Sector	**Público**	**Sector**	**Público**	
N.º	15	10	0	1	2
Percentagem	89,29%		3,57%		7,14%



- **Síntese das opiniões**

Relativamente às opiniões discordantes, essas referem que os respectivos conteúdos devem ser entregues à Assembleia Legislativa para serem debatidos, a fim de estarem em harmonia com as linhas governativas da RAEM e elevar o nível de reconhecimento e de aceitação.

Análise e resposta

Os regulamentos administrativos complementares a elaborar pelo Governo, que definem as atribuições e o funcionamento da Comissão Permanente para a Cibersegurança e o Centro de Alerta e Resposta a Incidentes de Cibersegurança, bem como a designação das entidades públicas responsáveis pela sua supervisão baseiam-se nas competências que lhes são conferidos pela Lei n.º 13/2009 *(Regime jurídico de enquadramento das fontes normativas internas, aprovados após apreciação da Assembleia Legislativa)*, na qual está previsto que a matéria relativa à estrutura orgânica interna do governo pode ser regulamentada pelo regulamento administrativo.

Breve conclusão

As opiniões dos sectores e o público, em generalidade, não têm queixas em relação à essa matéria. O Governo irá empenhar-se à elaboração dos respectivos regulamentos administrativos para regular o funcionamento das instituições em causa.

Parte III

Opiniões e sugestões não mencionadas no documento de consulta

No processo da consulta pública da "Lei da Cibersegurança", os diversos sectores e o público apresentaram muitas opiniões e sugestões não mencionados no documento de consulta, enumerando-se, de seguida, as opiniões e sugestões mais relevantes para efeitos de análise.

1. Melhoramento da consciencialização da cibersegurança junto da sociedade e do público

Há muitas opiniões que consideram que deve incluir-se toda a população e os turistas no âmbito de aplicação da "Lei da Cibersegurança", pelo que todas as entidades e pessoas de Macau têm a responsabilidade de proteger a sua própria segurança da rede.

Análise e resposta

A "Lei da Cibersegurança" visa principalmente a criação de um sistema de gestão administrativa com carácter de protecção da segurança cibernética, regulando claramente os deveres e responsabilidades dos operadores das infra-estruturas críticas; por isso, os destinatários desta lei são os operadores das infra-estruturas críticas e não quaisquer das empresas ou indivíduos. O trabalho legislativo e a implementação da "Lei da Cibersegurança" carecem dos esforços conjuntos do Governo e dos diversos sectores da sociedade para proceder à sua concretização, os serviços governamentais relacionados prosseguirão acções específicas de divulgação e sensibilização. Com a entrada em funcionamento do CARIC, serão divulgadas informações atinentes à cibersegurança de Macau junto da sociedade, no sentido de reforçar a consciência de protecção da cibersegurança de todos os sectores e as camadas sociais, alcançando aos objectivos de uma protecção eficaz da cibersegurança.

2. Certificação e classificação de segurança dos equipamentos

Os diversos sectores propõem ao Governo a implementação da certificação de segurança dos equipamentos críticos e dos produtos específicos para cibersegurança e introduzir um mecanismo de classificação e de níveis sobre os fornecedores ou empreiteiros que prestem serviços de cibersegurança.

Análise e resposta

O fulcro da cibersegurança reside no regime regular e eficaz de gestão dos sistemas informático e de rede, no procedimento de operação e nas medidas para prevenção e resposta, não sendo o essencial os equipamentos usados ou serviços prestados pelos fornecedores; assim, o que se pretende é que, através do estabelecimento do regime e medidas de carácter permanente e específico previstas na "Lei da Cibersegurança", se possam detectar com a maior antecedência, as anomalias da cibersegurança e estabelecer medidas de aperfeiçoamento correspondentes, com finalidade de garantir a segurança cibernética.

3. Conteúdo das orientações para os operadores das infra-estruturas críticas

O público considera que deve publicar o conteúdo das orientações para os operadores das infra-estruturas críticas emitidas pelo Governo e as especificações e funções dos equipamentos de monitorização para uso na "Lei da Cibersegurança".

Análise e resposta

As entidades supervisoras emitirão as respectivas orientações aos operadores das infra-estruturas críticas em conformidade com as situações específicas dos diversos sectores; para esse efeito, o Governo promoverá, através de vários meios, a comunicação com esses sectores, de modo a implementar efectivamente a cibersegurança. No entanto, visto que os conteúdos dessas orientações envolvem provavelmente a operação concreta das suas actividades sectoriais e as informações internas destas actividades sectoriais, o Governo terá de actuar cautelosamente quanto à sua revelação, citando-se como exemplo as especificações dos equipamentos de vigilância e as suas funcionalidades, que não convém ser reveladas, caso contrário poderá levar-se a maior vulnerabilidade a ataques cibernéticos.

4. Coordenação dos critérios de supervisão da cibersegurança

Há opiniões que propõem que o acto de definir as orientações para uso sectorial pode ser precedido da recolha das opiniões pelas entidades supervisoras junto dos respectivos sectores, assegurando-se, assim, a sua praticabilidade e a viabilidade das mesmas e a harmonização dos critérios de supervisão da cibersegurança aquando da sua aplicação.

Análise e resposta

A "Comissão Permanente para a Cibersegurança", o "Centro de Alerta e Resposta a Incidentes de Cibersegurança" e as entidades supervisoras em diversos domínios, irão colaborar com as instituições operadoras das infra-estruturas críticas dos respectivos domínios, definir consoante a situação concreta os regimes de gestão da cibersegurança, os procedimentos de operação e critérios concretos da cibersegurança adequados para esses sectores, bem como proceder oportunamente à sua revisão e actualizações em conformidade com a evolução das tecnologias. Além disso, o CARIC prestará instruções técnicas necessárias e realizará cursos de formação adequados para as entidades supervisoras e supervisionadas, enquanto as entidades supervisoras, ao implementarem os critérios de supervisão da cibersegurança para os diversos domínios, assegurarão a coordenação e harmonização desses critérios juntamente com o CARIC.

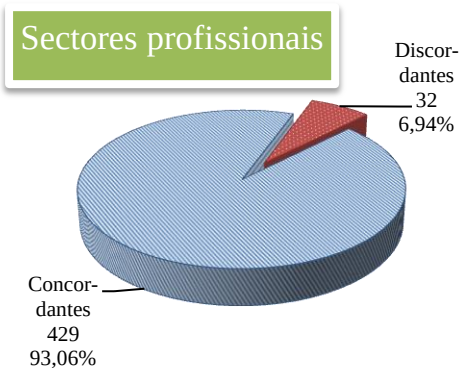
Parte IV

Conclusão

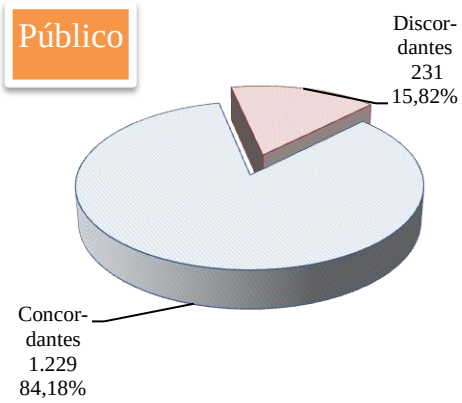
Os trabalhos de consulta pública da "Lei da Cibersegurança" da RAEM foram concluídos com sucesso, pelo que o Governo da RAEM agradece sinceramente a todos os sectores e o público pelas valiosas opiniões manifestadas durante o processo da consulta pública, por essas terem contribuído positivamente para o aperfeiçoamento do conteúdo do projecto de lei.

Muitos serviços públicos intervieram e participaram no processo da consulta pública da "Lei da Cibersegurança", sendo os elementos da equipa de trabalho para tal efeito provenientes de 14 serviços, órgãos e entidades públicos, a saber, o Gabinete do Secretário para a Segurança, a Direcção dos Serviços de Administração e Função Pública, a Direcção dos Serviços de Economia, a Direcção dos Serviços de Assuntos Marítimos e de Água, a Direcção dos Serviços para os Assuntos de Tráfego, o Gabinete para o Desenvolvimento do Sector Energético, a Direcção dos Serviços de Protecção Ambiental, a Autoridade de Aviação Civil, a Autoridade Monetária de Macau, a Direcção de Inspecção e Coordenação de Jogos, o Instituto para os Assuntos Cívicos e Municipais, os Serviços de Saúde, a Direcção dos Serviços de Correios e Telecomunicações e a Polícia Judiciária, bem como foram recolhidas opiniões e marcada a participação activa do Gabinete para a Protecção de Dados Pessoais nas sessões da consulta pública. Tudo isto evidencia a importância que o Governo tem dado à tarefa do estabelecimento do sistema de protecção da cibersegurança.

A consulta pública da "Lei da Cibersegurança" tem como objectivo auscultar amplamente as opiniões dos cidadãos, de forma a chegar a um consenso na sociedade. Sintetizadas as opiniões recolhidas, o Governo da RAEM fica a conhecer que as opiniões dos sectores e do público mostram concordância, na generalidade, com o rumo legislativo e o conteúdo proposto da "Lei da Cibersegurança", e as suas sugestões valiosas contribuem significativamente para o melhoramento e aperfeiçoamento do projecto de lei.



Opiniões dos Sectores profissionais



Opiniões do Público

Simultaneamente com o processo da organização do presente relatório de consulta, o Governo da RAEM iniciou o trabalho da elaboração e aperfeiçoamento do projecto de "Lei da Cibersegurança", tendo procedido à revisão dos seus conteúdos com base nas opiniões recolhidas na consulta pública, procurando tornar mais claro o teor textual da lei, para reduzir o mal entendimento do público e, assim, alcançar o consenso de toda a população neste projecto de lei, e no futuro, cumprir em conjunto esta lei, para consolidar a cibersegurança da sociedade.