

**Consulta Pública sobre
a Lei da Cibersegurança da
Região Administrativa
Especial de Macau**

Gestão da cibersegurança

Modelo de funcionamento da supervisão da cibersegurança

COMISSÃO PERMANENTE PARA A CIBERSEGURANÇA



CARIC



Entidades supervisoras dos diversos domínios

Sector público

SAFP

Sector privado

IACM
AMCM
DICJ
DSE
SS
DSAMA
DSAT
GDSE
DSPA
AAC
CTT

Modelo de funcionamento da supervisão da cibersegurança

SAFP

Supervisiona

Todos os órgãos, serviços e entidades públicos (excepto a PJ e os CTT)

IACM

Supervisiona

Operadores de abate de animais em matadouros legais, abastecimento público grossista de produtos alimentares sujeitos a controlos sanitários e fitossanitários

AMCM

Supervisiona

Bancos, entidades financeiras, instituições de seguros

DICJ

Supervisiona

Operadores de jogos de fortuna ou azar em casino

DSE

Supervisiona

Operadores de abastecimento grossista de combustíveis

SS

Supervisiona

Hospitais privados

DSAMA

Supervisiona

Operadores de portos, transportes marítimos e abastecimento de água

(Cont.)

Modelo de funcionamento da supervisão da cibersegurança

(Cont.)

DSAT

Supervisiona

Operadores de transportes terrestres

GDSE

Supervisiona

Operadores de fornecimento e distribuição de energia eléctrica e de gás natural

DSPA

Supervisiona

Operadores de tratamento de águas residuais, recolha e tratamento de resíduos

AAC

Supervisiona

Operadores de transportes aéreos

CTT

Supervisiona

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 do serviço das redes públicas

Modelo de funcionamento da supervisão da cibersegurança

Comissão Permanente para a Cibersegurança

- Órgão decisório no topo hierárquico, ao qual compete definir a orientação geral, os objectivos e as estratégias no âmbito da cibersegurança;
- Discutir sobre as propostas de definição ou alteração, bem como as opiniões e informações respeitantes ao diploma da cibersegurança;
- Acompanhar a situação da cibersegurança entre os operadores das infraestruturas críticas;
- Apreciar e deliberar sobre o relatório geral da cibersegurança;
- Emitir orientações para o “Centro de Alerta e Resposta a Incidentes de Cibersegurança” e para as entidades de supervisão.



Modelo de funcionamento da supervisão da cibersegurança

Centro de Alerta e Resposta a Incidentes de Cibersegurança

- Órgão de coordenação operacional de nível intermédio, composto pela Polícia Judiciária, Direcção dos Serviços de Administração e Função Pública e Direcção dos Serviços de Correios e Telecomunicações;
- Conforme a prática comum a nível internacional, monitorizar o tráfego de dados informáticos na forma de linguagem máquina (códigos de instrução 0 e 1), entre os sistemas informáticos das infraestruturas críticas e a internet e, se necessário, supervisionar em tempo real a dimensão do fluxo dos dados e as características dos datagramas, com a finalidade de prevenir, detectar e combater ataques e invasões cibernéticas;
- Reagir a incidentes de cibersegurança, promover os deveres e medidas relativos à cibersegurança;
- Definir padrões, instruções e procedimentos das acções de alerta e resposta a incidentes;
- Emitir alertas sobre incidentes de cibersegurança;
- Prestar o apoio técnico às entidades de supervisão e supervisionadas.

Modelo de funcionamento da supervisão da cibersegurança

Entidades de supervisão nos diversos domínios

- Cabe à Direcção dos Serviços de Administração e Função Pública supervisionar os serviços públicos;
- Compete a onze serviços públicos supervisionar os operadores das infraestruturas críticas do sector privado;
- Definir o regime de gestão da cibersegurança para os operadores sujeitos à sua supervisão;
- Definir e promover as orientações para os procedimentos de resposta às emergências;
- Recolher os relatórios sobre a cibersegurança dos operadores sujeitos à sua supervisão;
- Monitorizar o cumprimento das regras de cibersegurança.



Consulta Pública sobre a Lei da Cibersegurança

Convidamos sinceramente as individualidades dos diversos sectores a apresentarem, por escrito, as suas sugestões ou opiniões sobre o conteúdo do presente documento de consulta:

Período de consulta:

11 de Dezembro de 2017 a 24 de Janeiro de 2018

Meios de apresentação das sugestões ou opiniões:

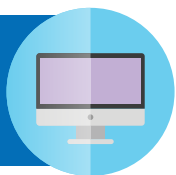
Por carta



Através do correio ou entrega directa:
ao Gabinete do Secretário para a Segurança, sito na Calçada dos Quartéis da RAEM, ou
à Direcção dos Serviços da Administração e Função Pública, sita na Rua do Campo, nº 162, Edifício "Administração Pública", 27º andar.

Por favor especifique na capa o seguinte: "Sugestões e Opiniões sobre a Lei da Cibersegurança"

Por via electrónica



Através do acesso à página electrónica específica no Portal do Governo da Região Administrativa Especial de Macau (www.gov.mo) ou no *website* do Gabinete do Secretário para a Segurança (www.gss.gov.mo/pt/ciberseg)