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

Deveres e responsabilidades sobre cibersegurança

Deveres de cibersegurança

Deveres dos operadores das infraestruturas críticas

Deveres de carácter orgânico

- Criar unidades especializadas na gestão da cibersegurança e designar os respectivos responsáveis;
- Proceder à verificação de antecedentes (vetting) de idoneidade e experiência profissional dos responsáveis e técnicos em lugares-chave;
- Estabelecer mecanismos e meios para apresentar reclamações e denúncias relacionadas com a cibersegurança.

Deveres de cibersegurança

Deveres dos operadores das infraestruturas críticas

Deveres de carácter procedimental, preventivo e reactivo

- Estabelecer o regime de gestão da cibersegurança e os procedimentos operacionais internos;
- Implementar medidas internas de protecção, monitorização, alerta e resposta às emergências de cibersegurança;
- Informar o "Centro de Alerta e Resposta a Incidentes de Cibersegurança" da ocorrência de incidentes, dando conhecimento do facto à respectiva entidade de supervisão e desenvolver as acções de resposta à emergência.

Deveres de cibersegurança

Deveres dos operadores das infraestruturas críticas

Deveres de auto-avaliação e relato

- Proceder, com o próprio pessoal ou com a intervenção de entidades profissionais a quem deleguem, a avaliação da segurança da própria rede e dos riscos, e submeter um relatório à respectiva entidade de supervisão.

Dever de colaboração

- Aquando da verificação do cumprimento dos deveres de carácter procedimental, preventivo e reactivo, facultar a entrada do pessoal do “Centro de Alerta e Resposta a Incidentes de Cibersegurança” ou da respectiva entidade de supervisão nas suas instalações, e disponibilizar-lhes as informações necessárias para efeitos de fiscalização.

Deveres de cibersegurança

Deveres dos operadores das infraestruturas críticas

Deveres específicos dos operadores da rede pública

- Solicitar aos utentes os dados de identificação verdadeiros (“Real Name System”), na altura da celebração de contratos ou da confirmação da prestação de serviços para acesso à rede, registo de nomes de domínio, serviços das redes públicas de telecomunicações fixas ou móveis;
- Conservar, durante um ano, os registos WebLogs das translações entre os endereços IP internet e os endereços das redes internas, ao disponibilizarem aos utentes serviço de acesso à internet. (Proceder à reserva de registos WebLogs).

Funcionamento do "Real Name System"

- O pessoal dos operadores da rede ao disponibilizar serviços aos seus utentes deve solicitar-lhes os dados de identificação, os quais devem ser conservados na instituição em causa e regulados pela "Lei da Protecção de Dados Pessoais";

- Este regime não afecta o acesso à rede em Macau dos cartões SIM comprados no exterior pelos turistas (por exemplo os serviços de roaming).

Sanções administrativas a aplicar aos operadores das infraestruturas críticas que não cumprem os deveres

Sanções principais

O incumprimento dos deveres constituirá infracção administrativa a ser punida com pena de multa, sem prejuízo da responsabilidade penal prevista na demais legislação e regulamentação.

Se não houver risco material nem reincidência, aplica-se apenas a advertência, caso o infractor consiga a sanação, no prazo fixado, das irregularidades.

Sanções acessórias

Pelos actos graves, poderão ainda ser aplicadas, separada ou cumulativamente:

- A privação do direito à participação em concursos públicos para aquisição de bens e serviços, abertos por entidades públicas;
- A privação do direito aos subsídios ou benefícios concedidos por entidades públicas;
- A suspensão, parcial ou total, da eficácia da autorização, licença, contrato de concessão ou alvará.

Responsabilidades disciplinares do pessoal dos órgãos públicos no âmbito da cibersegurança

Responsabilidades disciplinares

Relativamente ao incumprimento dos deveres de cibersegurança no âmbito dos órgãos públicos, nomeadamente quando a situação é gerada, por dolo ou negligência, dos seus dirigentes ou responsáveis, os mesmos terão de assumir responsabilidades disciplinares conforme o estipulado no Regime Jurídico da Função Pública.

Data de entrada em vigor da "Lei da Cibersegurança"

A lei entra em vigor 30 dias após a sua publicação.

Para que os operadores da rede disponham de um período de preparação suficiente, é estipulada uma outra data para a entrada em vigor do "Real Name System" e da conservação dos "WebLogs".

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)