(Tradução)

Assunto: Resposta à interpelação escrita apresentada pelo Deputado à Assembleia Legislativa, Mak Soi Kun

Na sequência da interpelação escrita apresentada pelo Deputado Mak Soi Kun, no dia 17 de Maio de 2021, enviada a coberto do ofício da Assembleia Legislativa n.º 606/E432/VI/GPAL/2021, de 28 de Maio de 2021, recebido pelo Gabinete do Chefe do Executivo a 31 de Maio de 2021, após auscultar a Polícia Judiciária, cumpre a este Gabinete apresentar a seguinte resposta:

Relativamente à criação do mecanismo de gestão e resposta de riscos de cibersegurança em Macau, mencionada na presente interpelação, o Governo da RAEM já concluiu vários trabalhos para aperfeiçoar os diplomas legais, as estruturas organizacionais, os apoios técnicos, a gestão e resposta, por forma a criar um sistema de gestão preventiva eficaz da cibersegurança, bem como aumentar de forma contínua a capacidade de prevenção e resposta a riscos existentes nas redes de internet.

A "Lei da cibersegurança" que entrou em vigor em 2019 e os respectivos regulamentos administrativos complementares determinam expressamente os deveres e as responsabilidades dos operadores de infra-estruturas críticas e das partes intervenientes na área da cibersegurança. Simultaneamente, prevêem a criação da Comissão para a Cibersegurança (CPC), responsável pela vertente da política e estratégia geral do trabalho relativo à cibersegurança da RAEM, do Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC), responsável pelo trabalho em matéria de alerta e resposta a incidentes de cibersegurança, assim como das entidades de supervisão de cibersegurança (entidades de supervisão), às quais compete supervisionar e zelar pelo cumprimento dos deveres de cibersegurança por parte dos operadores. O CARIC continua a colaborar estreitamente com as entidades de supervisão, os operadores e com todos os sectores da sociedade, dando apoio aos operadores no cumprimento dos deveres impostos pela lei através dos técnicos e profissionais e por meio do sistema de acompanhamento da situação de cibersegurança e de outros dispositivos, de *hardware* e *software* modernos. Ao mesmo tempo, o CARIC já definiu as medidas concretas a serem tomadas pelos operadores no cumprimento dos deveres legais, assim como os seus procedimentos e requisitos, prestando apoio às partes intervenientes na realização e promoção do trabalho de criação do sistema da cibersegurança de Macau.

Quanto à previsão e avaliação do impacto causado por ataques cibernéticos, mencionada na interpelação, o CARIC já divulgou, em Maio do ano passado, a

(Tradução)

"Regulação de padrões de gestão da cibersegurança", exigindo que os operadores cumpram os deveres legais, procedendo à classificação do nível de protecção da cibersegurança e à avaliação de risco de acordo com a importância de diferentes redes e sistemas informáticos para o bem-estar social, segurança ou ordem pública ou interesse público, implementando as medidas de segurança consoante o respectivo nível das redes e sistemas informáticos, de modo a evitar ao máximo possível os incidentes de cibersegurança como a fuga de dados, bem como adquirindo a capacidade técnica de recuperação rápida do funcionamento do sistema após a ocorrência de incidentes. Os operadores necessitam, ainda, de realizar regularmente o teste de segurança destinado às redes e sistemas fundamentais, com vista a melhorar constantemente o nível de protecção da segurança.

No que diz respeito ao plano de contingência para incidentes da cibersegurança, é estabelecido, no documento "Regulação de alerta, resposta e comunicação de incidentes da cibersegurança", emitido pelo CARIC, um mecanismo de coordenação recíproca, entre o CARIC, as entidades supervisoras e os operadores, acerca da emissão de alertas e recepção de comunicação dos incidentes, bem como são dadas aos operadores instruções gerais para prevenção e resposta a incidentes de cibersegurança. Ao mesmo tempo, é previsto na referida Regulação que os operadores devem, consoante a situação real do funcionamento da sua actividade, elaborar planos de resposta a diversos incidentes, bem como realizar acções de formação e ensaios de forma periódica, no intuito de conseguir dar resposta a casos emergentes e minimizar o impacto por eles gerado.

Com o objectivo de aperfeiçoar o nível de coordenação entre os serviços e entidades interessadas e a sua capacidade técnica de resposta a incidentes da cibersegurança, no dia 11 de Dezembro do ano transacto, o CARIC realizou, em colaboração com todas as entidades de supervisão e alguns dos operadores, o primeiro simulacro de incidente, depois da entrada em vigor da Lei da cibersegurança. Consequentemente, deu-se um impulso para que todas as partes participantes dominassem cada procedimento no âmbito da resposta ao incidente, tendo-se também efectuado uma revisão do mecanismo para a sua optimização. Futuramente, o CARIC irá continuar a promover os simulacros juntamente com os operadores dos diversos sectores e as respectivas entidades de supervisão, conjugando esforços para aumentar o nível geral de Macau em matéria de resposta aos incidentes de cibersegurança.

A Chefe do Gabinete do Secretário para a Segurança
Cheong Ioc Ieng
17 de Junho de 2021