(Tradução)

Assunto: Interpelação escrita apresentada pelo Deputado à Assembleia Legislativa, Leong Hong Sai

Na sequência da interpelação escrita apresentada pelo Deputado Leong Hong Sai, de 30 de Agosto de 2022, enviada a coberto do ofício da Assembleia Legislativa n.º 879/E669/VII/GPAL/2022, de 6 de Setembro de 2022, e recebida pelo Gabinete do Chefe do Executivo em 6 de Setembro de 2022, após auscultar a Polícia Judiciária (PJ) e a Direcção dos Serviços de Administração e Função Pública (SAFP), cumpre a este Gabinete apresentar a seguinte resposta:

Com vista à melhor protecção das redes, sistemas e dados informáticos dos operadores de infra-estruturas críticas de Macau, no domínio do sistema jurídico, a Região Administrativa Especial de Macau (RAEM) elaborou e foi implementada, em 2019, a Lei n.º 13/2019 (Lei da Cibersegurança), na qual se prevê explicitamente que os operadores de infra-estruturas críticas devem cumprir os deveres e as responsabilidades em matéria da manutenção da situação da sua própria cibersegurança. Além disso, foram promulgadas, em Maio de 2020, a Regulação de padrões de gestão da cibersegurança e a Regulação de alerta, resposta e comunicação de incidentes da cibersegurança, que visam estabelecer, de forma mais concreta, as medidas, os procedimentos e as exigências no cumprimento dos deveres de cibersegurança pelos operadores de infra-estruturas críticas nos termos da Lei da Cibersegurança. Na área da garantia organizacional, o Governo da RAEM criou também, para entrar em vigor no mesmo dia da entrada em vigor dos diplomas legais acima referenciados (22 de Dezembro de 2019), um sistema de cibersegurança da RAEM, composto pela Comissão para a Cibersegurança e pelo Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC), que é coordenado pela Polícia Judiciária e integra a Direcção dos Serviços de Administração e Função Pública, a Direcção dos Serviços de Correios e Telecomunicações e as Entidades de Supervisão de Cibersegurança, criando-se assim nos termos da lei, progressivamente, um mecanismo de trabalho que é presidido pela Comissão para a Cibersegurança e com a

(Tradução)

colaboração estreita do CARIC, das Entidades de Supervisão de Cibersegurança e dos operadores de infra-estruturas críticas.

De acordo com a Lei da Cibersegurança, e tal como exigido pelas referidas normas técnicas, todos os serviços públicos locais têm de implementar adequados planos de emergência de resposta a incidentes de cibersegurança e de concretizar, a nível organizacional e técnico, os trabalhos de prevenção antecipada, de fiscalização durante a ocorrência do incidente e de melhoramento após o incidente, do âmbito de cibersegurança, para formarem um círculo fechado no âmbito da gestão da cibersegurança e para poderem proteger efectivamente os sistemas informáticos dos serviços públicos, incluindo as informações que envolvem a segurança do Estado. Quanto ao nível organizacional, é exigida a necessidade de indicar responsáveis pela cibersegurança, de implementar políticas internas e instruções de trabalho, no âmbito da cibersegurança, e de proceder à distribuição adequada de funções para o sistema informático e o trabalho de cibersegurança, ao passo que, a nível técnico, exige-se que se proceda à classificação de acordo com a importância dos sistemas informáticos da rede e se adoptem medidas técnicas de cibersegurança do correspondente grau de intensidade, incluindo a construção do *firewall*, *intrusion detection and prevention systems*, *security gateway*. A este nível exige-se também a actualização antecipada, em termos de segurança, dos equipamentos de *software* e *hardware*, entre outras, para se defender dos ataques dos *hackers* externos, bem como a obrigação de se distribuírem apropriadamente aos trabalhadores as competências para uso do sistema, de acordo com o "*principle of least privilege*", de criar boas estratégias de *password* e registos de auditoria das operações do *log* para poderem prevenir os acessos, por usurpação de poder, e as alterações não autorizadas dos dados informáticos por parte dos trabalhadores internos, entre outros. Por outro lado, todos os serviços públicos têm de, nos termos da lei, proceder anualmente à avaliação de risco da sua situação de cibersegurança e entregar um relatório anual às Entidades de Supervisão de Cibersegurança a que pertencem.

(Tradução)

Desde a implementação da Lei da Cibersegurança, que os mecanismos de trabalho no âmbito da cibersegurança de Macau têm tido continuamente um bom funcionamento e produzido os efeitos esperados. De acordo com as informações fornecidas pelos SAFP, os serviços públicos de Macau têm efectuado o trabalho relativo à defesa da cibersegurança em conformidade com a Lei da Cibersegurança e as exigências das normas técnicas acima referidas. O Governo da RAEM também procede, em tempo oportuno, ao acompanhamento e à apreciação dos planeamentos da cibersegurança dos serviços públicos e da sua eficácia de execução, bem como fornece os apoios técnicos correspondentes. Até hoje, não houve nenhum caso em que os serviços públicos tenham sido punidos, de acordo com a lei, pelas entidades de supervisão por causa de violação dolosa ou incumprimento dos deveres de cibersegurança.

Quanto à intensificação do conceito de cibersegurança dos trabalhadores, os SAFP referiram que têm continuamente fornecido acções de formação e workshops nesse âmbito aos trabalhadores de diferentes áreas e categorias, incluindo as acções de formação na vertente prática e operacional, tais como o "Curso de Sensibilização sobre Cibersegurança", o "Cursos de Formação Técnica sobre Conta Única de Acesso Comum", para que os trabalhadores responsáveis pela execução e operação possam utilizar os correspondentes sistemas de forma correcta e intensificar o conceito de cibersegurança. Ao mesmo tempo, na vertente técnica e de gestão, foram organizados vários cursos, nomeadamente, "CISP-A", "Curso de Certificação de CISP (Macau)", "Curso de Segurança da Aplicação *Web*", "Curso de Cibersegurança e Desenvolvimento de Actividades", "*Workshop* temático sobre a Governação Electrónica – Desenvolvimento de Sistemas Informáticos e Gestão do Sistema da Rede Informática", com vista a aprofundar os conhecimentos dos trabalhadores sobre o desenvolvimento, manutenção e funcionamento dos sistemas informáticos.

Além disso, o CARIC tem organizado periodicamente diversas actividades de divulgação e educação e acções de formação profissional para os operadores de infra-

(Tradução)

estruturas críticas, incluindo os serviços públicos, bem como realiza anualmente exercícios de incidentes de cibersegurança, para melhorar as capacidades do pessoal no âmbito da gestão da segurança informática e resposta a incidentes súbitos de cibersegurança.

O Chefe do Gabinete do Secretário para a Segurança, substituto

Chang Cheong

22 de Setembro de 2022