Desenvolver gradualmente as actividades de gestão para colaborar na implementação da Lei da Cibersegurança

No dia 25 de Novembro de 2019 foi publicado o Regulamento Administrativo n.º 35/2019 (Comissão para a Cibersegurança, Centro de Alerta e Resposta a Incidentes de Cibersegurança e entidades de supervisão de cibersegurança) que complementa a composição e funcionamento do sistema de cibersegurança da RAEM constante da Lei n.º 13/2019 (Lei da cibersegurança). Ambos os diplomas vão entrar oficialmente em vigor no dia 22 de Dezembro de 2019, o que significa que Macau já possui as bases necessárias na legislação e no enquadramento institucional para desenvolver a gestão de cibersegurança. No futuro, sob a liderança e supervisão da Comissão para a Cibersegurança (CPC), o Centro de Alerta e Resposta a Incidentes de Cibersegurança (CARIC), as entidades de supervisão de cibersegurança (entidades de supervisão) e os operadores de infra-estruturas críticas (operadores) irão desempenhar as suas funções nos termos da lei, e esforçar-se em conjunto por assegurar a cibersegurança de Macau e ajudar a defender a segurança global do País.

I. Acções prioritárias a serem desenvolvidas

1. Lista concreta referente à designação dos operadores privados de infra-estruturas críticas

Após a entrada em vigor da Lei da Cibersegurança e dos regulamentos administrativos complementares, as 11 entidades de supervisão irão elaborar uma lista concreta agregada dos operadores privados, legalmente sujeitos à respectiva supervisão, a dita lista depois de ser apreciada, discutida e reconhecida pela CPC será publicada, por Despacho Regulamentar Externo do Chefe do Executivo. Os operadores supervisionados devem cumprir, de acordo com as exigências da legislação e entidades de supervisão, os respectivos deveres consagrados pela Lei da Cibersegurança. Caso os operadores privados indicados na referida lista, a publicar no futuro, preencham as circunstâncias estipuladas no artigo 5.º da Lei da Cibersegurança, podem requerer isenção junto do Chefe do Executivo.

2. Apresentação de parecer sobre a idoneidade da pessoa a ser designada como principal responsável pela cibersegurança e o seu substituto

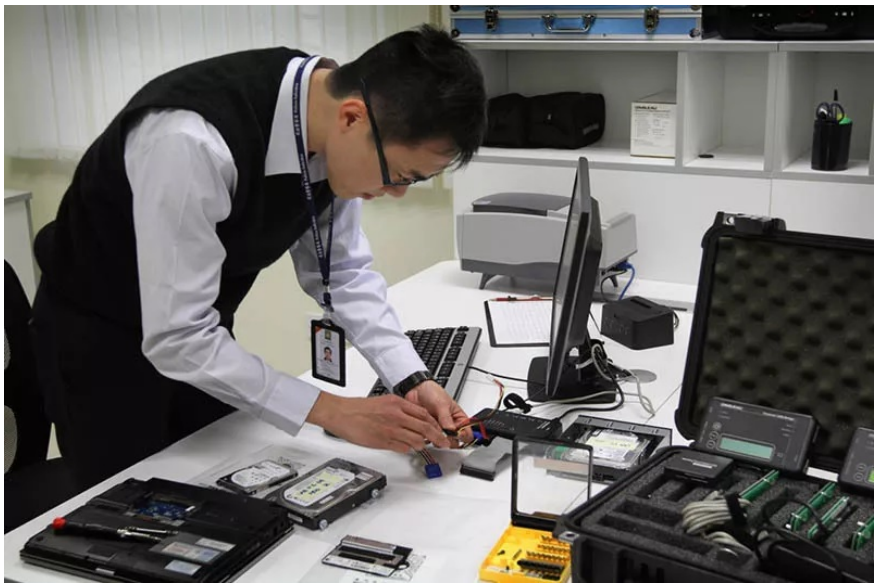
Conforme o disposto no artigo 10.º da Lei da Cibersegurança, fixam-se os deveres de carácter orgânico a que estão sujeitos os operadores privados, entre os quais se exige a solicitação de parecer à Polícia Judiciária sobre a idoneidade e eventuais impedimentos relativos às pessoas que pretendam designar como principal responsável pela cibersegurança e o respectivo substituto.

Para tal, a PJ está a elaborar instruções que regulam os procedimentos de consulta, designadamente quanto à forma de entrega de informação por parte dos operadores privados, tipos de informação necessária e vias de resposta aos operadores. Por outro lado, a PJ irá colaborar com as entidades de supervisão de diversos sectores e domínios, às quais caberá uniformizar e coordenar a realização dos respectivos trabalhos cujos resultados serão divulgados aos operadores quando for oportuno.

3. Emissão de normas técnicas relativas à gestão de cibersegurança

Nos termos do disposto na Lei da Cibersegurança e nos regulamentos administrativos complementares, as entidades de supervisão são serviços e organismos da Administração Pública, aos quais cabe supervisionar, nos termos da lei, as actividades dos operadores em matéria da cibersegurança e zelar pelo cumprimento dos respectivos deveres.

No sentido de disponibilizar apoio às entidades de supervisão no exercício das suas competências, o "grupo de trabalho interdepartamental para a definição de padrões de cibersegurança" composto pela Polícia Judiciária, a Direcção dos Serviços de Administração e Função Pública e a Direcção dos Serviços de Correios e Telecomunicações, já elaborou os textos relativos às respectivas normas técnicas, incluindo a "Regulação de padrões de gestão da cibersegurança" e a "Regulação de alerta, resposta e comunicação a incidentes de cibersegurança", os quais constituem a base fundamental para os futuros operadores que realizem actividades de cibersegurança (como a determinação do nível de protecção de segurança, a avaliação de risco, a apresentação de relatórios anuais, a resposta e comunicação de incidentes e outros). Foram realizadas duas rondas de consultas sobre os textos de normas técnicas com as entidades de supervisão, os respectivos textos oficiais vão ser concluídos em breve, e depois de serem apreciados pela Comissão e a lei entrar em vigor, serão divulgados aos operadores pelas entidades de supervisão.



As duas normas técnicas acima referidas são os requisitos e padrões mínimos no âmbito de gestão de cibersegurança, e podem ser aplicáveis tanto aos operadores públicos como aos privados. Tendo em consideração os riscos de cibersegurança enfrentados por cada sector, as entidades de supervisão considerem, sempre que necessário, as características e condições do sector em que as suas supervisadas trabalhem, com vista a definir, por si próprias, as suas normas técnicas com base nas orientações das duas normas técnicas comuns, para atingir os requisitos inerentes à gestão de cibersegurança exigidos pelos relativos sectores.

4. Implementação ordenada dos regulamentos pertinentes ao Real-Name System dos cartões telefónicos

O artigo 24.º da Lei da Cibersegurança, que define o Real-Name System dos cartões telefónicos, deverá estar plenamente implementado a partir de 20 de Abril de 2020, ou seja, após o prazo de 120 dias a contar da data de entrada em vigor da Lei da Cibersegurança. Entretanto, os utilizadores de cartões pré-pagos, devem registar a identidade nos operadores de serviços de telecomunicações móveis aos quais pertencem, durante o período de transição compreendido entre o dia 22 de Dezembro de 2019 em que a Lei da Cibersegurança inicia a produção de efeitos e o dia 19 de Abril de 2020; depois deste período, os cartões pré-pagos em uso só vão ser reactivados quando os utilizadores fizerem os registos de identidade. Face a essa necessidade, a Direcção dos Serviços de Correios e Telecomunicações e os operadores de telecomunicações já desenvolveram os equipamentos necessários, os sectores envolvidos vão dar as informações e os respectivos arranjos sobre este assunto em tempo oportuno, com vista a ajudar os utilizadores de cartões pré-pagos nesta tarefa.

II. Realização progressiva da gestão da cibersegurança

Após a entrada em vigor da Lei da Cibersegurança e dos regulamentos administrativos complementares, os trabalhos acima referidos irão ser, gradualmente, desenvolvidos pelas entidades de supervisão e pelos operadores de infra-estruturas críticas, consoante as directrizes no âmbito da gestão de cibersegurança em Macau definidas pela CPC. Por outras palavras, os intervenientes irão, conforme as exigências da mesma lei, realizar progressivamente as actividades da respectiva gestão, com vista a reforçar, incessantemente, a capacidade de protecção no aspecto da cibersegurança de Macau e prevenir diversos riscos desta área, garantindo a segurança e o bom funcionamento das redes e dos sistemas informáticos das infra-estruturas críticas.