Governo do Estado de Roraima
Polícia Civil do Estado de Roraima
"Amazônia: patrimônio dos brasileiros"

MEMORANDO Nº 99/2021/POLICIA CIVIL/DENARC/GAB

Boa Vista/RR, 03 de setembro de 2021.

Ao Senhor
Amauri de Oliveira Carvalho
Escrivão de Polícia

Assunto: Resposta(faz)

Senhor,

Em resposta ao Evento 2000405, encaminho o questionário abaixo seguido das respostas solicitadas.

Informamos ainda que encaminharemos este processo à DG para conhecimento.

Atenciosamente,

(assinado digitalmente)

DARLINDA DE MOURA SANTOS VIANA

Delegada de Polícia Civil

Diretora do Denarc/ Titular do DERCC.

Questionário:

Sobre unidades especializadas no combate aos crimes cibernéticos:

1. Qual a história de criação da unidade? O Distrito Estadual de Repressão à Crimes Cibernéticos – DERCC foi criado através do Decreto n. 29.637-E de 03 de dezembro de 2020, e a regulamentação de suas atribuições foi feita por Resolução do Conselho Superior de Polícia (Resolução n. 002/2021-CONSUPOL, de 21 de abril de 2021). A primeira servidora lotada foi a DPC DARLINDA DE MOURA SANTOS VIANA, como titular da unidade em 01/06/2021, respondendo cumulativamente com a atividade principal Direção do Departamento de Narcóticos. Por meio de remanejamento interno do Denarc, foi lotado mais três servidores (agentes de polícia), todos com formação em Tecnologia da Informação.

2. Qual a formação e composição dos seus quadros funcionais? Existem apenas profissionais da segurança pública ou são contratados consultores? Todos os servidores tem formação na área de Sistemas de Informação (TI), inclusive a Delegada Titular. Todos os servidores são policiais civis, e não há consultores contratados, mas nada impede essa forma de auxílio.

3. Qual a infraestrutura, tecnologias e equipamentos disponíveis? A unidade ainda está sendo equipada.

4. Quais os treinamentos (em tecnologia) necessários e/ou disponíveis para que sejam parte da unidade? Não há requisito legal para lotação de servidor na DERCC, entretanto, por questões gerenciais, foram lotados na unidade apenas servidores formados em alguma área de TI. Além da

formação, os servidores serão submetidos a treinamento especifico de investigação cibernética e segurança de redes.

5. A unidade tem algum tipo de sistema “principal” para combate ao crime? Não

6. Existem ferramentas que tenham sido desenvolvidas internamente? Quem faz o apoio e suporte de TI? Há ferramentas em desenvolvimento. A própria equipe com ajuda de integrantes de Agência de Inteligência de Roraima.

7. Existe um perfil profissional específico ou desejado para se trabalhar numa unidade desse tipo? O perfil do profissional para essa unidade são servidores obstinados, persistentes, detalhistas, com conhecimento técnico e voltado ao aprendizado contínuo.

8. Qual o número de registros de ocorrência por mês? Quantas são lavradas na própria unidade? Quantas são online? É possível ter uma ocorrência oriunda de outras unidades da estrutura de segurança pública? Ocorrências de crimes virtuais

9. Existe uma estatística sobre o tempo médio de uma investigação considerando a abertura de uma ocorrência e sua conclusão? Não.

10. Existem trabalhos ou mapas de análise estatística do tipo “Mancha Criminal”? Talvez algum tipo de abordagem por tipo de crime e frequência de determinados tipos de ocorrência p.ex.? Não.

11. Dentre os vários crimes elucidados certamente existem aqueles de maior destaque e que viraram casos de estudo e análise. Poderiam ser citados e resumidas algumas dessas ações? Por sigilo de investigação, os métodos e procedimentos usados não podem ser divulgados (artigo 20, parágrafo único, do Código de Processo Penal).

12. A unidade faz ações educacionais ou patrocina ações de prevenção ou monitoração de crimes digitais ou cibercrimes? Sim. Há sempre divulgação via mídia sociais da Polícia Civil de Roraima, em forma de “cards”, para indicar novos golpes e meios de proteção. Além de inserção em mídia tradicional.

13. A unidade faz consultoria para outros órgãos de governo ou da iniciativa privada na parte de segurança da informação ou na parte de tecnologia de prevenção a crimes digitais? Não.

Sobre Crimes Digitais: 1. Existem dados (Bancos de dados ou microdados) que possam ser analisados para fins estatísticos? Como posso solicitar o acesso? Existem, mas os microdados são protegidos por sigilo e não podem ser divulgados ou ter acesso externo aos Bancos.

2. Quais são os Modus Operandi mais comuns? Quais os crimes mais denunciados? Uso de redes sociais e internet para cometimento de crime. Perfil fake de rede social, Crimes contra Honra cometidos por redes sociais, “Porno revenge”, “Sexestorsão”, Golpe OLX, Golpe do Whats falso.

3. Qual o típico perfil do criminoso? Depende do crime.

4. Existem indicativos de organizações criminosas “tradicionais” migrando para atuar nesse tipo de crime? Sim.

5. Existe um levantamento sobre o perfil das vítimas? Não

6. Existe uma tabela com a tipificação dos crimes? Sim.

7. A tipificação (tipificação criminal de delitos informáticos –Lei nº 12.737, de 30 de novembro de 2012) é suficiente para os casos ou é necessário fazer também um trabalho de analogia com os outros tipos de crime previstos no código penal para a devida instrução processual e apresentação de denúncia? Não abrange todos os tipos de conduta, sendo necessário o uso da norma penal comum para tipificação da maioria dos crimes.

8. Como se combatem as quadrilhas virtuais e como fica a tipificação criminal frente aos diferentes tipos de ações e responsabilidades? Existem casos que possam ser analisados (Por exemplo: Quem faz o vírus, quem faz o site ou hospeda o site para golpes, quem compartilha, quem usa a máquina infectada, quem recebe e repassa o ganho ilícito)? As Associações criminosas (antigas Quadrilhas ou bandos) são identificadas, coletado o material de prova (materialidade), sua individualização de conduta nos atos praticados e devidamente indiciados, um a um. São enquadrados como co-autores ou partícipes, bem como incluídos nas tipificações para Associação criminosa ou organização criminosa, conforme o caso.

9. Como é tratada a divulgação de crimes realizados para recrutamento por facções ou por demonstração de força? É tratado como “Promoção de Organização Criminosa”, previsto no tipo penal 2º da lei 12.850/2013 com pena de reclusão de 3 a 8 anos.

10. Qual é o protocolo de combate a divulgação, venda e entrega de armas, drogas e entorpecentes? Existem casos que possam ser analisados? Não podem ser divulgados em razão do sigilo de investigação (artigo 20, parágrafo único, do Código de Processo Penal)

Sobre os aspectos jurídicos nos crimes via web: 1. Como é resolvida ou tratada a questão da jurisdição em investigações de crimes que são ou podem ser executados em vários locais pelo mundo (Estado/Brasil/Mundo)? Crimes transnacionais são de competência da Justiça federal e portanto, atribuição da Polícia Federal (CC 150.629/SP, Rel. Ministro NEFI CORDEIRO, TERCEIRA SEÇÃO, julgado em 22/02/2018, DJe 28/02/2018).

2. Existem acordos de cooperação policial no Brasil para esse tipo de crime? Qual o protocolo adotado para se acionar outras forças da área de segurança? Não há formalização de cooperação entre as Pcs neste aspecto, mas há cooperação de fato. Apenas o contato direto entre unidades policiais.

3. Caso o Brasil venha a aderir, qual a expectativa sobre a aplicação da “Convenção de Budapeste” no referente ao combate ao cibercrime e ao crime digital? A melhor expectativa possível em razão das facilidades de acesso a provas e provedores situados em outros países, sem necessidade de acordo de cooperação internacional preestabelecido ou intermediação de terceiros envolvidos na investigação.

4. A lei 13.964/2019 (Lei Anticrime), que possibilitou a infiltração virtual de agentes policiais para obter dados de conexão e cadastrais de membros de organizações envolvidas com crimes cibernéticos já foi usada em algum caso? Podem ser resumidas para ilustração? Não.

5. Imaginando que a unidade tem participação na Estratégia Nacional de Segurança Cibernética (batizada de "E-Ciber" por meio do decreto 10.222), já existem ações efetivas que possam ser destacadas? Está em desenvolvimento alguns programas de desenvolvimento em governança de Ti da PCRR.

6. Entre os casos de sucesso, existem histórias de ações conjuntas com outras unidades policiais do BRASIL ou do mundo em ações de combate ao cibercrime e crime digital? Não

7. Tendo as empresas privadas de tecnologia como a Google e Microsoft entre outras, além de ONGs (SaferNet p.ex.) exercido um papel expressivo no combate e sobretudo na denúncia de crimes pela internet, como é a cooperação com a iniciativa privada? Existem protocolos definidos? Sim. Sim.

8. Existem eventos do tipo “Lei 9099” (Baixo Potencial Ofensivo) que podem ser ou foram resolvidos por Termos Circunstanciados com o escopo dos crimes digitais? Sim.

Documento assinado eletronicamente por **Darlinda de Moura Santos Viana**, **Delegada de Polícia**, em 03/09/2021, às 09:03, conforme Art. 5º, XIII, "b", do Decreto Nº 27.971-E/2019.

A autenticidade do documento pode ser conferida no endereço https://sei.rr.gov.br/autenticar informando o código verificador **2835842** e o código CRC **D9222E10**.
