Sobre Unidades especializadas no combate aos crimes cibernéticos

1. Qual a história de criação da unidade?

Foi criada em 2020. Faz parte da estrutura da DEIC

2. Qual a formação e composição dos seus quadros funcionais? Existem apenas profissionais da segurança pública ou são contratados consultores?

Servidores policiais civis

3. Qual a infraestrutura, tecnologias e equipamentos disponíveis?

Estrutura básica, sem equipamentos avançados

4. Quais os treinamentos (em tecnologia) necessários e/ou disponíveis para que sejam parte da unidade?

Não há treinamento institucional, o policial deve ter conhecimento prévio na área

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?

Não. Suporte de TI fornecido pelo Estado

7. Existe um perfil profissional específico ou desejado para se trabalhar numa unidade desse tipo?

Conhecimento prévio na área e disponibilidade de horário

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?

Todos os registros de Boletins de Ocorrência envolvendo crimes ocorridos por meio virtual são encaminhados a Delegacia Especializada, independente da Delegacia de Polícia de registro.

Atualmente, por limitação da estrutura de Unidades de Polícia em nosso sistema, não temos como especificar os registros feitos pela própria Delegacia de Combate a Crimes de Informática, entretanto, já estão sendo tomadas as medidas necessárias para a solução dessa limitação.

	2019								2020												2021					
REG - Sistema de Origem	mai	jun	jul	ago	set	out	nov	dez	jan	fev	mar	abr	mai	jun	jul	ago	set	out	nov	dez	jan	fev	mar	abr	mai	jun
Totais	1.684	2.186	2.806	2.820	3.022	3.426	3.199	2.852	3.910	3.656	2.315	677	1.016	1.440	1.256	1.236	3.287	6.361	6.653	5.792	6.288	6.395	7.075	6.895	7.207	325
Delegacia Virtual (online)	1	-	4	2	-	9	7	1	3	4	32	178	181	231	187	120	1.731	4.228	4.229	3.944	4.186	3.995	4.680	4.328	4.173	180
Delegacias de Polícia (presencial)	1.683	2.186	2.802	2.818	3.022	3.417	3.192	2.851	3.907	3.652	2.283	499	835	1.209	1.069	1.116	1.556	2.133	2.424	1.848	2.102	2.400	2.395	2.567	3.034	145

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

Sim

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.?

Sim

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?

Clonagem de sim card (chip) de prefeitos do interior de SC. A investigação culminou com a prisão de 4 pessoas em São Luís/MA

12.A unidade faz ações educacionais ou patrocina ações de prevenção ou monitoração de crimes digitais ou cibercrimes?

Realizava palestras em escolas antes da pandemia

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?

Consultoria apenas para outras unidades policias

Sobre Crimes Digitais

1. Existem dados (Bancos de dados ou microdados) que possam ser analisados para fins estatísticos? Como posso solicitar o acesso?

Sim.

2. Quais são os Modus Operandi mais comuns? Quais os crimes mais denunciados?

Os crimes mais denunciados são Estelionato, Ameaça, Injúria, Difamação, Calúnia e Invasão de dispositivo informático

3. Qual o típico perfil do criminoso?

jovem com conhecimento em tecnologia

4. Existem indicativos de organizações criminosas "tradicionais" migrando para atuar nesse tipo de crime?

Não

5. Existe um levantamento sobre o perfil das vítimas?

Geralmente pessoas com alto poder aquisitivo e com pouca instrução em tecnologia

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?

Necessário realizar um trabalho de analogia com os outros tipos de crimes previstos no código penal.

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)?

Sem casos a serem analisados

9. Como é tratada a divulgação de crimes realizados para recrutamento por facções ou por demonstração de força?

Sem casos a serem analisados

10.Qual é o protocolo de combate a divulgação, venda e entrega de armas, drogas e entorpecentes? Existem casos que possam ser analisados?

sem casos a serem analisados

Sobre os aspectos legais 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 (RJ/Br/Mundo)?

Art. 70, §4º, CPP

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?

Acordo de Cooperação Jurídica em Matéria Penal – MLTA com o Ministério da Justiça e países signatários;

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?

Aperfeiçoamento legislativo

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?

Sigiloso

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?

Não

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?

Sim

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?

A iniciativa privada não tem interesse em fornecer subsídios necessários para elucidação dos crimes virtuais, haja vista que o compartilhamento de IP's por CGNat sem a identificação da porta lógica pelos provedores tem dificultado a individualização dos criminosos. Ademais, as empresas de telefonia não se cercam de cuidados para a inserção fraudulenta de dados em sim cards (chips) o que proporciona uma maior impunidade

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, no caso de crimes contra a honra praticados em ambiente virtual.

Respeitosamente,