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

3. Qual a infraestrutura, tecnologias e equipamentos disponíveis?

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

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

6. Existem ferramentas que tenham sido desenvolvidas internamente? Quem faz o apoio e suporte de TI?

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

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?

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

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.?

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?

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

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?

Sobre Crimes Digitais

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

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

3. Qual o típico perfil do criminoso?

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

5. Existe um levantamento sobre o perfil das vítimas?

6. Existe uma tabela com a tipificação dos crimes?

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?

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)?

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

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

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?

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?

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?

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?

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?

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?

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?

Resposta

01- Resposta: A Delegacia de Repressão a Crimes Cibernéticos foi criada através da PORTARIA SSP Nº 350, DE 19 DE ABRIL DE 2017 e subornada à Diretoria de Policia Civil da Capital. Atualmente, passou a ser chamada de Divisão Especializada em Repressão a Crimes Cibernéticos – DRCC e está subordinada à Diretoria de Repressão à Corrupção e ao Crime Organizado – DRACCO.

02 - . Resposta: 02 Delegados de Polícia, 02 Escrivães de Polícia, 02 Agentes de Polícia, 01 Analista em TI e 01 Assistente Administrativo.

03 - Resposta: Uma sala para cada um dos delegados, uma sala para investigação e uma sala para registro de ocorrências e oitivas.

04 - Resposta: Não há requisito para ingresso nesta divisão, entretanto, após o ingresso a própria equipe da divisão passa acompanhar e auxiliar os novos integrantes para que possam desenvolver suas atividades. Ademais, existe o curso ministrado pela Academia de Polícia Civil que visa criar uma base mínima sobre o conhecimento da área.

05 - Resposta: Não há um sistema principal.

06 - Resposta: Não há um sistema desenvolvido internamente. A parte técnica dos equipamentos é de

responsabilidade da área de TI da SSP.

07 - Resposta: O perfil desejado é de alguém que tenha conhecimento básico ou básico/avançado em Tecnologia da Informação.

08 - Resposta: Em média 100; Em média 30; Atualmente, por conta da pandemia COVID-19, as ocorrências têm sido registradas no site Delegacia Virtual, dessa forma, a maioria dos BOs atuais são registrados online; É possível sim, pois após registro das ocorrências os delegados recebem os BOs para despachar, momento em que podem verificar se tratar de um crime de responsabilidade desta divisão, então esses BOs são recebidos.

09 - Resposta: A confecção de um Boletim de Ocorrência completo com print's e provas anexadas levam em média 1 hora. A investigação de um crime cibernético é muito mais demorada, mas na média, considerando Pedido de Quebra de Sigilo, encaminhamento e retorno de Ofícios requisitórios, identificação da materialidade e individualização dos autores, leva em média 03 meses de investigação cada caso. Há casos que são elucidados em menos de um mês, há casos que levam anos.

10 - Resposta: A divisão não realiza esse tipo de estatística, o crime mais comum nesta divisão é o ESTELIONATO (golpe).

11 - Resposta: Operação Ostentação: Os AUTORES furtavam dinheiro da conta bancárias das vítimas e compravam bens para ostentar, mais informações podem ser obtidas em https://surgiu.com.br/2018/05/08/policia-civil-do-tocantins-deflagra-operacao-ostentacao-em-palmas-e-goiania/ ou https://conexaoto.com.br/2018/10/10/policia-civil-paulista-apreende-milhoes-de-reais-em-bens-a-partir-de-investigacoes-da-policia-civil-do-tocantins; Operação Perfil Oculto: AUTORES se passam por mulheres e trocam fotos intimas com homens, posteriormente passam a extorquir a vítima para que não divulguem as fotos íntimas obtidas, mais informações em https://www.to.gov.br/ssp/noticias/operacao-perfil-oculto-da-policia-civil-do-tocantins-resulta-na-prisao-de-tres-pessoas-suspeitas-de-extorsao-praticada-via-internet-no-rio-grande-do-sul/24fq2pdkojsw ou https://conexaoto.com.br/2020/07/06/operacao-da-policia-civil-resulta-na-prisao-de-tres-pessoas-suspeitas-de-extorsao.

12 - Resposta: Os delegados constantemente produzem vídeos educativos alertando a população, os quais são divulgados principalmente via WhatsApp e nos Jornais locais, bem como, a Diretoria de Comunicação da SPP produz e divulga matérias educativas. Não há consultoria por parte da divisão.

01 - Resposta: Por motivo de sigilo dos dados sensíveis, não há disponibilização de banco de dados com as informações questionadas.

02 - Resposta: O crime mais comum e denunciado é o ESTELIONATO(golpe). Os ESTELIONATOS não são estáticos, assim que um tipo de golpe fica conhecido, os autores migram para outro tipo de golpe, sendo que posteriormente retornam para o golpe inicial.

03 - Resposta: Não foi feito analise criminológica do perfil dos criminosos.

04 - Resposta: Embora algumas facções criminosas estejam praticado extorsão e estelionato por meio virtual, não é possível afirmar que estejam "migrando" para o cometimento de crime por meio virtual. Aparentemente trata – se de mais uma forma utilizada por eles.

05 - Resposta: Não foi feito analise criminológica do perfil dos vitimas.

06 - Resposta: O enquadramento dos fatos, a tipificação criminal, é feita após a análise de cada caso.

07 - Resposta: A lei em questão trata de "Invasão de dispositivo informático", "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", "Falsificação de documento particular" e "falsificação de cartão". Nesta divisão os crimes mais comuns são ESTELIONATO, EXTORSÃO, FURTO(MEDIANTE FRAUDE), dessa forma a minoria dos crimes comunicados amoldam – se à lei 12.737 de 30 de Novembro de 2012.

08 - Resposta: O combate as quadrilhas especializadas em crimes virtuais é feito de forma pontual e a tipificação e

responsabilização também se dá de acordo com o caso concreto.

09 - Resposta: Não há casos registrados nesta divisão para os crimes citados.

10 - Resposta: Não há casos registrados nesta divisão para os crimes citados.

Sobre os aspectos legais nos crimes via web

01 - Resposta: A divisão segue o preconizado no Código de Processo Penal. Há crimes em que a investigação deve ser feita pela Delegacia mais próxima ao endereço residencial da vítima, outros crimes são de responsabilidade do local da obtenção da vantagem.

02 - Resposta: Em caso de necessidade de cooperação de forças de segurança fora da nossa jurisdição, podemos acionar o Ministério da Justiça para intermediar a referida interlocução.

03 - Resposta: A expectativa é que com a adesão tenhamos maior facilidade de atuação em crimes que por sua própria natureza transcendem as fronteiras geográficas.

04 - Resposta: Ainda não foi utilizada infiltração virtual.

05 - Ainda não há ações efetivas que possam ser destacadas

06 - Resposta: Operação Ostentação com apoio da Polícia Civil de SÃO PAULO, GOIÁS e CiberLab do Ministério da Justiça; Operação Perfil Oculto com apoio da Polícia Civil de RIO GRANDE DO SUL.

07 - Resposta: Google, Microsoft, WhatsApp, Facebook, Instagram fornecem plataforma para contato direto, entretanto, não há possibilidade de solicitação de dados ou informações relevantes sem que haja uma Decisão Judicial de Quebra de Sigilo de Dados

08 - Resposta: A portaria de criação da Divisão Especializada em Repressão a Crimes Cibernéticos-DRCC preconiza que esta não investigará crimes com penas inferiores a 04 anos, entretanto, algumas investigações já foram finalizadas nesta divisão por conta da complexidade investigativa.

Encerrada a presente manifestação

Clique aqui para responder à **Pesquisa de Satisfação**

Agradecemos a sua participação.
Sistema de Ouvidorias do Poder Executivo Federal
https://falabr.cgu.gov.br/

Mensagem Automática
Favor não responder a este e-mail.