



DCCIBER

DIVISÃO DE CRIMES CIBERNÉTICOS



**DEIC - POLÍCIA
CIVIL DE SÃO
PAULO**



CRIAÇÃO

A Divisão de Crimes Cibernéticos foi criada pelo Decreto N° 65.241, de 13 de outubro de 2020 tendo como escopo apurar fraudes praticadas por meios eletrônicos, com o envolvimento de organizações criminosas ou com o emprego de recursos de alta tecnologia.



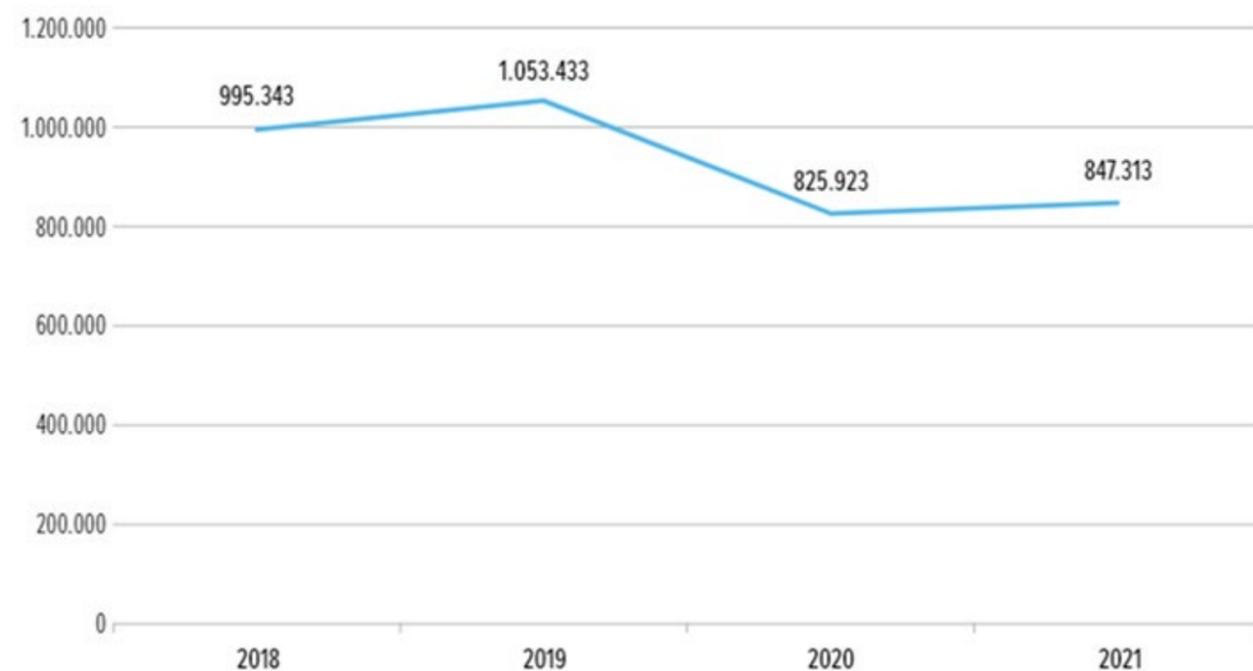


CENÁRIO: CRIMINALIDADE E VIOLÊNCIA

Anuário Brasileiro de Segurança Pública 2022

GRÁFICO 23

Roubo e furto de celulares
Brasil, 2018 – 2021

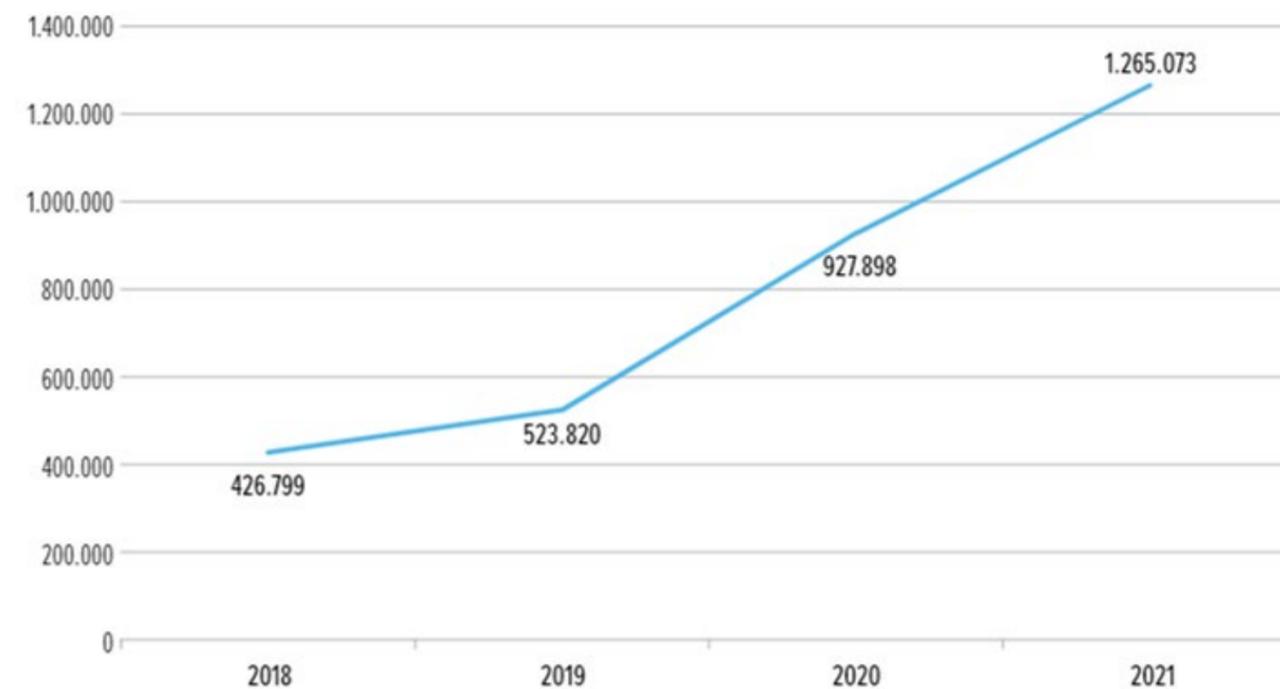


Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Polícia Civil do Distrito Federal; Polícia Civil de Minas Gerais; Instituto de Segurança Pública/RJ (ISP); Instituto Brasileiro de Geografia e Estatística (IBGE); Fórum Brasileiro de Segurança Pública.

Anuário Brasileiro de Segurança Pública 2022

GRÁFICO 24

Número de registros de estelionato
Brasil, 2018 – 2021



Fonte: Secretarias Estaduais de Segurança Pública e/ou Defesa Social; Polícia Civil do Distrito Federal; Polícia Civil de Minas Gerais; Instituto de Segurança Pública/RJ (ISP); Instituto Brasileiro de Geografia e Estatística (IBGE); Fórum Brasileiro de Segurança Pública.





ORGANOGRAMA

DIVISÃO DE CRIMES CIBERNÉTICOS

Assistência Policial

LAB - TAC - Laboratório Técnico de Análises Cibernética

CIC - Centro de Inteligência Cibernética

1ª DELEGACIA DE POLÍCIA

Fraudes Contra Instituições Financeiras praticadas por Meios Eletrônicos

2ª DELEGACIA DE POLÍCIA

Fraudes Contra Instituições de Comércio Eletrônico praticadas por Meios Eletrônicos

3ª DELEGACIA DE POLÍCIA

Violação de Dispositivos Eletrônicos e Redes de Dados

4ª DELEGACIA DE POLÍCIA

Lavagem e Ocultação de Ativos Ilícitos praticadas por Meios Eletrônicos



EFETIVO E CAPACIDADE TÉCNICA

EFETIVO DA DIVISÃO

83 Policiais, sendo

10 DELEGADOS

19 ESCRIVÃES

38 INVESTIGADORES

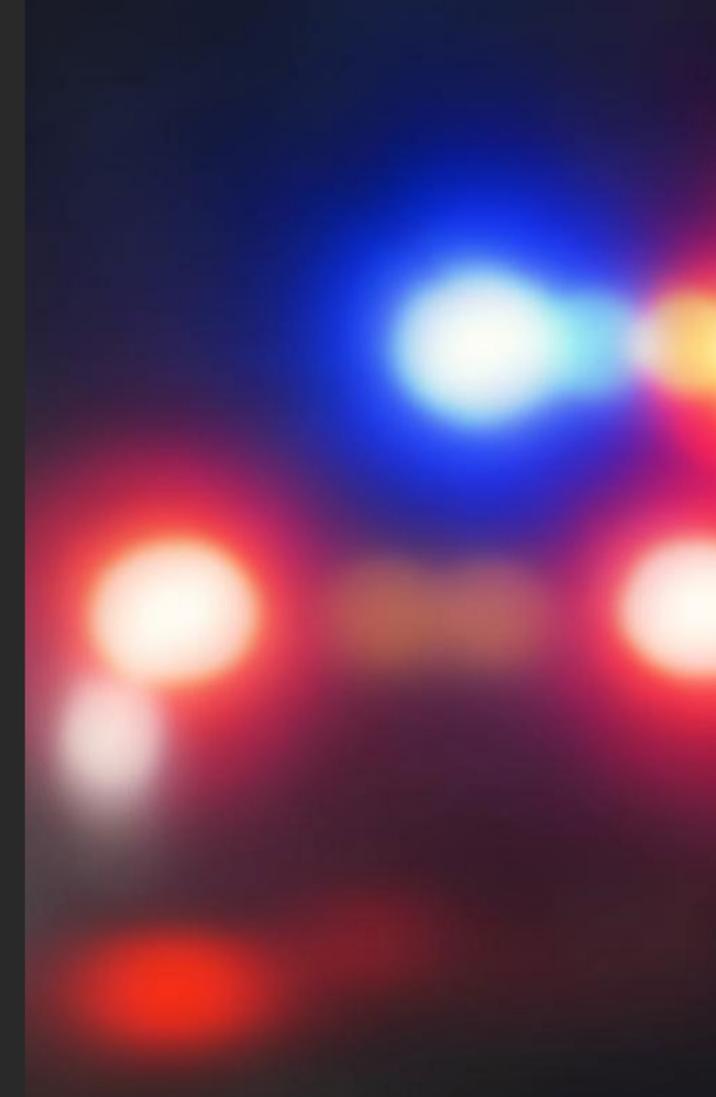
12 AGENTES POLICIAIS

02 AGENTES DE TELECOM

02 AUXILIAR DE PAPILOSCOPISTAS

CAPACITAÇÃO BÁSICA

- 1. INTERCEPTAÇÃO TELEMÁTICA**
- 2. CRIPTOMOEDAS**
- 3. INVESTIGAÇÃO EM FONTES ABERTAS**
- 4. META (Facebook, Instagram e Whatsapp)**
- 5. TREINAMENTO SOBRE PLD/CFT PARA OPERAÇÕES CAMBIAIS DE REMITTANCE**
- 6. SERVIÇO SECRETO EUA (TSA/HSI) - DARK WEB**
- 7. SISTEMA GUARDIÃO ONLINE**
- 8. CADEIA DE CUSTÓDIA (APREENSÃO, EXTRAÇÃO E ANÁLISE)**
- 9. CURSO PRÁTICO DE ANÁLISE DE RIF COAF**
- 10. LAVAGEM DE DINHEIRO POR MEIO DE CRIPTOMOEDAS**





DESAFIOS

- Troca de informações de inteligência
- Nivelamento das áreas jurídicas entre players e setores
- Trabalho em conjunto (estrutura hierárquica com atuação *adhocrática*)
- Estudos e desenvolvimentos de técnicas para combater fraudes





ROTINA DE ATENDIMENTO



01. Fraude

A empresa identifica a fraude e analisa as informações



02. Dados

A empresa realiza uma coleta completa dos dados gerados no sistema e armazena



03. Polícia Civil

A empresa procura a Polícia Civil para comunicar o fato.



04. Análise

Os dados são analisados junto a DCCIBER para enquadramento jurídico



05. Requerimento

Após o registro, a empresa oferece requerimento informando o ocorrido e fornecendo dados



06. CIC

Dados são analisados e processados pela empresa e pelo CIC



07. Investigação

Inicia-se a investigação com foco em medidas cautelares



08. Operações

Realização de operação policial para tratar o caso





DCCIBER EM NÚMEROS

OPERAÇÕES POLICIAIS - TOTAL ATÉ MAIO/2023

TOTAIS	OPERAÇÕES	MANDADOS	INDICIAMENTOS	CELULARES APREENDIDOS	OUTROS DISPOSITIVOS APREENDIDOS
1ª Delegacia	69	448	506	329	139
2ª Delegacia	31	171	156	123	59
3ª Delegacia	33	192	155	154	71
4ª Delegacia	52	481	292	250	67
TOTAL	239	1301	1109	856	336



DCCIBER EM NÚMEROS

VALORES APREENDIDOS E RECUPERADOS

Em razão das operações policiais e atividades desenvolvidas junto a Divisão de Crimes Cibernéticos do DEIC, foram apreendidos e recuperados bens e valores que totalizaram:

2022	36.963.645,00
2023	23.707.146,00

R\$ 60.670.791,00

(Sessenta milhões, seiscentos e setenta mil, setecentos e noventa e um reais)



P R E V E N Ç Ã O

PREVENÇÃO CORPORATIVA



PREVENÇÃO

CUIDADOS BÁSICOS DE UMA EMPRESA EM PREVENÇÃO CIBERNÉTICA

1. Firewall
2. Links redundantes
3. Backup apartado do sistema nativo ou em nuvem
4. Antivirus corporativo
5. Servidores de aplicação separados
6. Gestão da segurança da informação (compartimentação da informação)
7. Treinamento e capacitação continuada de pessoal
8. Programa de resposta a incidentes cibernéticos



Motivação dos cibercrimes: patrimônio

DESORDEM
MENTAL

INTERESSE
EMOCIONAL

INTERESSE
FINANCEIRO

POTENCIAIS ALVOS

PESSOA FÍSICA

PESSOA JURÍDICA





P R E V E N Ç Ã O

PREVENÇÃO PESSOAL



PREVENÇÃO Engenharia Social



**“- Look Bino...
It's a trap”...!!**



P R E V E N Ç Ã O

anatomia do golpe.....!



P R E V E N Ç Ã O

1. NÃO ATENDA NÚMEROS DESCONHECIDOS

2. NÃO RESPONDA MENSAGENS DE NÚMEROS DESCONHECIDOS

3. NÃO CLIQUE EM NENHUM LINK RECEBIDO



PREVENÇÃO

1. NÃO ATENDA NÚMEROS DESCONHECIDOS

Golpes mais comuns praticados por chamada de voz:

a. Falsa central de banco - violação de segurança

b. Falso escritório de advocacia - precatório

c. Falso INSS - liberação de benefício

d. Falso CDHU - negociação de dívidas



P R E V E N Ç Ã O

2. NÃO RESPONDA MENSAGENS DE NÚMEROS DESCONHECIDOS

Golpes mais comuns praticados por mensagens de aplicativos:

- a. “-Pai, faz um PIX pra mim...”
- b. Falsa campanha de ajuda
- c. Sextorsão
- d. Promoção de Hotéis e Restaurantes
- e. Premiações em geral (telefone, bolo, aniversário, viagens)



PREVENÇÃO

3. NÃO CLIQUE EM NENHUM LINK RECEBIDO

Golpes mais comuns praticados por ENVIO DE LINKS em aplicativos de comunicação:

- a. Mão fantasma - acesso remoto
- b. Phishing - captura de dados pessoais



DIVISÃO DE CRIMES CIBERNÉTICOS

dcciber.deic@policiacivil.sp.gov.br



Elaborado Por
Bruno Rechinho
Thiago Chinellato
Carlos Afonso Gonçalves da Silva