30955502 08027.000148/2025-14

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Assuntos Legislativos
Gabinete da Secretaria Nacional de Assuntos Legislativos
Área de Assessoria da Secretaria Nacional de Assuntos Legislativos

OFÍCIO Nº 250/2025/Assessoria-SAL/GAB-SAL/SAL/MJ

Brasília, na data da assinatura.

A Sua Excelência o Senhor
Deputado Federal Carlos Veras
Primeiro Secretário
Câmara dos Deputados
70160-900 - Brasília - DF

Assunto: Requerimento de Informação Parlamentar nº 510/2025, de autoria do Deputado Capitão Alberto Neto (PL/AM)

Referência: Ofício 1ªSec/RI/E/nº 49

Senhor Primeiro-Secretário,

Reporto-me ao Requerimento de Informação - RIC nº 510/2025, de autoria do Deputado Federal Capitão Alberto Neto (PL/AM), para encaminhar os seguintes documentos: (i) OFÍCIO Nº 116/2025/SEDIGI/MJ, elaborado pela Secretaria de Direitos Digitais (SEDIGI); (ii) OFÍCIO Nº 2166/2025/GAB-SENASP/SENASP/MJ e documento correlato, da lavra da Secretaria Nacional de Segurança Pública (SENASP), bem como (iii) OFÍCIO Nº 150/2025/GAB-SENACON/SENACON/MJ, e anexo, oriundos da Secretaria Nacional do Consumidor (SENACON), áreas técnicas deste Ministério da Justiça e Segurança Pública, a fim de subsidiar resposta ao i. parlamentar.

Na oportunidade, renovo protestos de estima e consideração.

Atenciosamente,

MANOEL CARLOS DE ALMEIDA NETO

Ministro de Estado da Justiça e Segurança Pública Substituto

Documento assinado eletronicamente por **Manoel Carlos de Almeida Neto**, **Ministro de Estado da Justiça e Segurança Pública - Substituto**, em 07/05/2025, às 17:06, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **30955502** e o código CRC **B4554994**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Anexos:

a) OFÍCIO Nº 116/2025/SEDIGI/MJ (30863304);
b) OFÍCIO Nº 2166/2025/GAB-SENASP/SENASP/MJ (30907541);
c) INFORMAÇÃO Nº 29/2025/CIBER-DIOPI/DIOPI/SENASP (30894397);
d) OFÍCIO Nº 150/2025/GAB-SENACON/SENACON/MJ (30941109), e
e) INFORMAÇÃO Nº 11/2025/CSA-SENACON/CGCTSA/DPDC/SENACON (30891734).

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 08027.000148/2025-14 SEI nº 30955502

Esplanada dos Ministérios, Bloco T, Ed. Sede, 4º Andar, Sala 436, - Bairro Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-3223 - www.gov.br/mj/pt-br
Para responder, acesse http://sei.protocolo.mj.gov.br

30863304 08027.000148/2025-14

Ministério da Justiça e Segurança Pública
Secretaria de Direitos Digitais

OFÍCIO Nº 116/2025/SEDIGI/MJ

Brasília, na data da assinatura.

À Senhora

BETINA GÜNTHER SILVA

Assessoria da Secretaria Nacional de Assuntos Legislativos

Assunto: Requerimento de Informação Parlamentar nº 510/2025, de autoria do Deputado Capitão Alberto Neto (PL/AM).

Senhora Assessora,

1. Em atenção ao Ofício 211 (30812731), que encaminha o Requerimento de Informação Parlamentar - RIC nº 510/2025, de autoria do Deputado Capitão Alberto Neto (PL/AM) -- o qual busca informações sobre as medidas adotadas pelo Ministério em face dos efeitos econômicos dos ataques cibernéticos de que sociedade civil brasileira tem sido vítima -, reitera-se o teor do Ofício 89 (30787624), por meio do qual esta Secretaria abordou a sua participação no combate a fraudes aplicadas pela internet. Como retratado naquele documento, esta Secretaria de Direitos Digitais (Sedigi) tem atuado, nesse contexto, de forma complementar às demais Secretarias.

2. Cumpre recordar que a Sedigi coordenou e acompanha a execução do Acordo de Cooperação nº 3/2024-MJSP/FEBRABAN, celebrado entre o Ministério da Justiça e Segurança Pública e a Federação Brasileira de Bancos (Febraban). A Sedigi também coordena o GT instituído para dar cumprimento ao objeto do referido acordo, que tem como objetivo a conjugação de esforços para articulação, formulação e desenvolvimento de estratégias de colaboração mútua voltadas à promoção de ações de prevenção e combate a fraudes, golpes e crimes cibernéticos.

3. No âmbito do GT, foi proposto o Projeto Aliança Nacional de Combate a Fraudes Bancárias Digitais, que se organizará em eixos temáticos, com base nos temas prioritários do Ministério da Justiça e Segurança Pública (MJSP). O projeto pretende oferecer uma resposta eficaz ao cenário de crescimento de crimes patrimoniais no ambiente digital, unindo esforços de atores com capacidade de empregar análise de dados e mantendo o cumprimento rigoroso de legislações de privacidade, como a Lei Geral de Proteção de Dados Pessoais (LGPD). O projeto visa a proteger não apenas a segurança e a proteção dos dados e do patrimônio dos indivíduos, mas também preservar a confiança dos usuários de internet e tornar o ambiente digital mais seguro e íntegro para transações e interações online.

4. Considerando ainda a relação existente entre a cultura de proteção de dados e a prevenção de fraudes, cumpre informar que a Sedigi exerce o papel de Presidente do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD), órgão de natureza consultiva, conforme o art. 3º, I, do Decreto nº 10.474, de 26 de agosto de 2020. Recomposto em 2024, o CNPD realizou três reuniões, todas no segundo semestre do ano. Com o propósito de otimizar os trabalhos e as entregas do CNPD, sete grupos de trabalho (GTs) foram criados, com destaque para o GT de educação e capacitação em proteção de dados. Com relação à Agenda Regulatória ANPD 2025-2026, foram votadas e deliberadas seis propostas, com destaque para as de (i) tratamento de dados de saúde; (ii) crianças e adolescente; (iii) definição de alto risco; (iv) regulação de critérios para reconhecimento e divulgação de regras de boas práticas e de governança; e (v) dados abertos, meio ambiente e proteção de dados.

5. Finalmente, acresça-se que, nos termos da Portaria de Pessoal SGD/MGI nº 4.987, de 16 de agosto de 2024, a Secretária de Direitos Digitais é a representante do Ministério da Justiça e Segurança Pública na Câmara-Executiva Federal de Identificação do Cidadão - Cefic. Ademais, preside o Comitê Gestor do Projeto Carteira de Identidade Nacional, no âmbito do Ministério da Justiça e Segurança Pública. Nesse sentido, destaca-se que a Nova Carteira de Identidade Nacional é considerada mais segura, porque contém novos elementos de segurança e reduz a possibilidade de emissão de um documento de identidade por unidade federativa -- passando a utilizar o CPF como número de registro nacional do brasileiro -, e também porque passa a contar com um código QR que permite a certificação fácil e confiável da sua validade [https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional/perguntas-frequentes-sobre-a-cin].

6. Seguimos à disposição para os esclarecimentos que se fizerem necessários.

Atenciosamente,

Nathalie Fragoso
Diretora de Programa
Secretaria de Direitos Digitais

Documento assinado eletronicamente por **Nathalie Fragoso e Silva Ferro**, **Diretor(a) de Programa**, em 05/03/2025, às 16:38, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **30863304** e o código CRC **31D08012**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 08027.000148/2025-14 SEI nº 30863304

Esplanada dos Ministérios, Bloco T, Ed. Sede, Sala 436, - Bairro Zona Cívico-Administrativa, Brasília/DF, CEP 70064-900
Telefone: (61) 2025-9481 / 3154 - www.gov.br/mj/pt-br
Para responder, acesse http://sei.protocolo.mj.gov.br

30891734 08027.000148/2025-14

Ministério da Justiça e Segurança Pública
Secretaria Nacional do Consumidor
Coordenação de Sanções Administrativas

INFORMAÇÃO Nº 11/2025/CSA-SENACON/CGCTSA/DPDC/SENACON

Processo nº: 08027.000148/2025-14

Assunto: Resposta ao Pedido de Informações

Referência: Requerimento de Informação nº 510/2025

Trata-se de Requerimento de Informação Parlamentar (RIC) nº 510/2025 (30812652), elaborado pelo Deputado Federal Capitão Alberto Neto, do PL/AM encaminhado a esta Secretaria Nacional do Consumidor (SENACON), do Ministério da Justiça e Segurança Pública (MJSP), por meio do qual são solicitadas informações a respeito do grande número de ataques cibernéticos no Brasil, nos seguintes termos abaixo:

> 1) Apesar dos alertas frequentes, quais medidas concretas foram implementadas pelo governo e empresas para fortalecer a segurança digital?
>
> 2) Como está a governança da segurança digital no setor público? Grandes órgãos estatais e empresas públicas realmente investem em infraestrutura cibernética ou a proteção digital ainda é negligenciada?
>
> 3) O Brasil está investindo em inteligência cibernética à altura da ameaça? Enquanto nações desenvolvidas destinam bilhões para defesa digital, o orçamento brasileiro para segurança cibernética está condizente com os riscos enfrentados?
>
> 4) Qual é o impacto na competitividade do Brasil? Se os ataques cibernéticos seguem atingindo bancos, indústrias e infraestrutura crítica, o país pode perder credibilidade internacional e afastar investidores?

Em atenção ao Requerimento de Informação Parlamentar, cabe inicialmente recordar que esta Secretaria Nacional do Consumidor (SENACON), do Ministério da Justiça e Segurança Pública (MJSP), é responsável por coordenar o Sistema Nacional de Defesa do Consumidor (SNDC), nos termos do art. 106 da Lei n.º 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor, CDC), e do art. 3º do Decreto n.º 2.181, de 20 de março de 1997. Tem por atribuições, entre outras, além de coordenar o SNDC, (i) adotar iniciativas de educação para o consumo e orientar os consumidores sobre seus direitos e garantias; (ii) monitorar o mercado de consumo; (iii) exercer advocacia normativa de interesse do consumidor; (iv) fiscalizar e aplicar as sanções administrativas previstas no CDC e em outras normas pertinentes à defesa do consumidor.

Na fiscalização das infrações às relações de consumo, todos os integrantes do Sistema Nacional de Defesa do Consumidor (SNDC) têm competência concorrente no exercício do poder de polícia administrativo, nos termos do art. 4º do Decreto n.º 2.181, de 1997. Cabe à SENACON, por meio do seu Departamento de Proteção e Defesa do Consumidor (DPDC), fiscalizar **as relações de consumo de relevante interesse geral e de âmbito nacional** e aplicar sanções administrativas previstas nas normas de defesa do consumidor, em conformidade com os artigos 55, § 1º, e 106, do Código de Defesa do Consumidor, e o art. 3º, inciso X, do Decreto n. 2.181, de 20 de março de 1997, bem como nos termos da Nota Técnica n. 328 – CGAJ/DPDC/2005. Nessa Nota, entendeu-se que, em relação às atribuições específicas do DPDC, a competência para o exercício do poder de polícia segue a distribuição constitucional das competências administrativas, em atendimento ao princípio da predominância do interesse, a justificar o escopo de atuação do órgão como restrito às relações de consumo de relevante interesse geral e de âmbito nacional. O interesse geral evidencia-se quando a causa transcende os interesses subjetivos das partes, ou seja, envolvem questões que se apresentam substancialmente relevantes para todo o País e repercutem em toda a sociedade. Esse entendimento foi institucionalizado, inclusive no Regimento Interno da Secretaria (Portaria MJ n.º 905, de 2017) e na Estrutura Regimental do MJSP, contida no Anexo I do Decreto nº 11.348, de 1º de janeiro de 2023.

Feita essa contextualização sobre a missão institucional da SENACON, passamos a endereçar os questionamentos apresentados.

No que se refere às medidas específicas implementadas para combater as fraudes praticadas pela internet, especialmente no comércio eletrônico, destaca-se a criação da Aliança Nacional de Combate a Fraudes Bancárias e Digitais, lançada em parceria com a Federação Brasileira de Bancos (Febraban), além da intensificação da fiscalização junto aos Procons e demais órgãos do Sistema Nacional de Defesa do Consumidor.

A Aliança está estruturada em três frentes de atuação:

a) Boas práticas para prevenção, detecção e resposta a fraudes;
b) Compartilhamento e tratamento de dados e informações;
c) atendimento a vítimas e capacitação de agentes.

Além disso, a SENACON também tem investido na modernização de seus sistemas de atendimento ao consumidor, fortalecendo a plataforma Consumidor.gov.br como ferramenta essencial para denúncias e resolução de conflitos. Outras medidas incluem a realização de campanhas educativas para conscientização da população sobre golpes virtuais, bem como a participação em grupos de trabalho interinstitucionais para aprimoramento da legislação e regulamentação do comércio eletrônico.

Quanto aos resultados obtidos até o momento com essa iniciativa, verifica-se uma maior coordenação entre os entes envolvidos, bem como a implementação de ações conjuntas de prevenção e repressão de fraudes digitais, de acordo com as diretrizes do Código de Defesa do Consumidor e da legislação correlata.

No que tange à existência de outras parcerias ou iniciativas em andamento visando à prevenção e repressão de crimes cibernéticos, destacam-se as colaborações com a Autoridade Nacional de Proteção de Dados (ANPD), a Secretaria de Operações Integradas (SEOPI) e a Polícia Federal, que desempenham papéis fundamentais na proteção dos consumidores e no combate aos crimes digitais.

Dentre os principais desafios enfrentados pelo Ministério na identificação e punição dos responsáveis por essas fraudes, citam-se a transnacionalidade dos delitos, a dificuldade de rastreamento das operações financeiras fraudulentas e a necessidade de cooperação com empresas do setor privado para o compartilhamento de informações.

Por fim, em relação às orientações e medidas preventivas divulgadas pelo Ministério para conscientizar e proteger os consumidores contra essas práticas fraudulentas, destacam-se campanhas educativas, cartilhas informativas e a realização de audiências públicas voltadas à transparência e ao empoderamento dos consumidores na luta contra fraudes digitais.

Apesar dos desafios, o Brasil tem um potencial significativo para avançar na segurança cibernética e fortalecer sua posição global. Com investimentos estratégicos, maior integração entre setores público e privado, e a promoção de uma cultura de inovação e segurança digital, o país pode transformar esses desafios em oportunidades.

Quanto aos canais de atendimento, a Senacon oferece vários instrumentos para que os consumidores possam fazer perguntas, registrar reclamações, denúncias e obter informações sobre questões relacionadas à proteção do consumidor. Aqui estão os principais canais de atendimento da Senacon: *site* oficial da Senacon, Plataforma de Atendimento ao Consumidor (Consumidor.gov.br), redes sociais, telefone e atendimento presencial, ouvidoria do Ministério da Justiça por meio da plataforma Fala.BR, dentre outros meios.

Observando que as reclamações ou demandas individuais de consumidores são de competência dos órgãos estaduais ou municipais do Sistema Nacional de Defesa do Consumidor (SNDC), esclarecemos que os consumidores devem procurar atendimento diretamente nas Secretarias de defesa do consumidor ou Procons locais. Alternativamente, recomenda-se o registro na plataforma Consumidor.gov.br, um serviço público alternativo para solução de conflitos de consumo que não substitui o serviço prestado pelos órgãos de defesa do consumidor. A partir desses registros, a Senacon realiza o monitoramento do mercado de consumo em nível nacional.

As políticas de proteção ao consumidor implementadas pelo Departamento de Proteção e Defesa do Consumidor (DPDC), no âmbito do Ministério da Justiça e Segurança Pública, contando com três principais bases de dados:

I - **Sistema Nacional de Informações de Defesa do Consumidor - Sindec:** política pública que, por meio de um conjunto de soluções tecnológicas, representa um eixo fundamental de integração do Sistema Nacional de Defesa do Consumidor (SNDC) e de fortalecimento da ação coordenada e harmônica entre seus órgãos.

II - ProConsumidor: sistema que está substituindo o Sindec, possibilita o monitoramento das ações implementadas pelos órgãos de estado ou entes de mercado, bem como subsidia a elaboração de estudos e pesquisas sobres os principais assuntos, problemas e fornecedores reclamados pelos consumidores. É um sistema simples, ágil e adaptado às necessidades atuais de atuação dos órgãos de defesa do consumidor, no atendimento aos consumidores, proporcionando o atendimentos célere e flexível.

III - **Consumidor.gov.br:** serviço público e gratuito que permite a comunicação direta entre consumidores e empresas para a solução de conflitos de consumo. Ele consiste em uma alternativa para o consumidor resolver seu problema diretamente com as empresas cadastradas, dispensada a intermediação de um representante do Estado. Esse serviço é monitorado pela Senacon, pelos Procons, Ministérios Públicos, Defensorias Públicas, Agências Reguladoras, entre outros órgãos, e também por toda a sociedade. Ele fornece ao Estado informações essenciais à elaboração e implementação de políticas públicas de defesa dos consumidores e incentiva a competitividade no mercado pela melhoria da qualidade e do atendimento ao consumidor.

A Senacon tem desenvolvido campanhas e iniciativas para fortalecer a proteção dos consumidores, utilizando seu site oficial, as redes sociais e o YouTube do Ministério da Justiça e Segurança Pública como principais canais de divulgação. Essas ações buscam ampliar a conscientização do público, garantindo que os consumidores estejam bem informados sobre seus direitos e saibam como se proteger contra fraudes na internet.

Importante destacar que a Secretaria Nacional do Consumidor (Senacon) lançou no ano passado o **Guia do Consumidor para a Black Friday,** um material informativo para ajudar os consumidores a realizarem compras seguras e evitarem golpes durante o evento promocional. Entre as principais orientações do guia, destaca-se a importância de verificar a procedência dos sites de compras eletrônicas antes de efetuar qualquer transação. Isso pode ser feito por meio de pesquisas sobre a reputação da loja, conferindo se há reclamações em plataformas como o Consumidor.gov.br e verificando se o site possui CNPJ ativo e canais de atendimento confiáveis.

Em síntese, esta Secretaria Nacional do Consumidor permanece acompanhando o fornecimento dos diferentes produtos e serviços no mercado de consumo, a fim de conferir a adequada proteção dos consumidores, por meio de diferentes instrumentos de política pública, a saber:

a) Educação para o consumo, por meio de eventos de formação e capacitação (https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/escola-nacional-endc);
b) Monitoramento de mercado, inclusive por meio de suas plataformas de atendimento aos consumidores, o SINDEC, o ProConsumidor e o consumidor.gov.br;
c) Advocacia normativa de interesse do consumidor;
d) Coordenação do Sistema Nacional de Defesa do Consumidor (SNDC), composto por órgãos e entidades públicas (PROCONs, Ministério Público, Defensoria Pública) e privadas (entidades civis de defesa do consumidor) de diferentes unidades da federação;
e) Articulação com os atores envolvidos com a temática (ministérios, agências reguladoras, representantes de consumidores e fornecedores);
f) Sanções administrativas.

Dito isso, seguimos à disposição para dialogar sobre a matéria em prol da efetiva proteção dos consumidores, bem como, havendo indícios de falhas no fornecimento de produtos e serviços no mercado de consumo, adotar medidas no âmbito desta Secretaria considerando os diferentes instrumentos de políticas públicas à disposição.

À consideração superior do GAB-DPDC, para ciência e, em caso de aquiescência, encaminhamento.

Respeitosamente,

LEONARDO AGUILAR VILLALOBOS

Coordenador-Geral de Consultoria Técnica e Sanções Administrativas, Substituto

Documento assinado eletronicamente por **LEONARDO AGUILAR VILLALOBOS**, **Coordenador(a)-Geral de Consultoria Técnica e Sanções Administrativas - Substituto(a)**, em 07/03/2025, às 21:14, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **30891734** e o código CRC **FB5DEB46**

O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Processo nº 08027.000148/2025-14 SEI nº 30891734

30894397 08027.000148/2025-14

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública
Diretoria de Operações Integradas e de Inteligência
Coordenação-Geral de Operações Integradas e Combate ao Crime Organizado

INFORMAÇÃO Nº 29/2025/CIBER-DIOPI/DIOPI/SENASP

Processo: **08027.000148/2025-14**

Assunto: **Requerimento de Informação Parlamentar n.º 510/2025, de autoria do Deputado Federal Capitão Alberto Neto (PL/AM).**

1. Trata-se de Requerimento de Informação Parlamentar n.º 510/2025 (30812652), de autoria do Deputado Federal Capitão Alberto Neto - PL/AM, o qual requer informações a respeito do grande número de ataques cibernéticos no Brasil, causando prejuízo de até R$ 2,3 trilhões na economia brasileira em 2024, conforme detalhado abaixo:

> 1. Apesar dos alertas frequentes, quais medidas concretas foram implementadas pelo governo e empresas para fortalecer a segurança digital?
>
> 2. Como está a governança da segurança digital no setor público? Grandes órgãos estatais e empresas públicas realmente investem em infraestrutura cibernética ou a proteção digital ainda é negligenciada?
>
> 3. O Brasil está investindo em inteligência cibernética à altura da ameaça? Enquanto nações desenvolvidas destinam bilhões para defesa digital, o orçamento brasileiro para segurança cibernética está condizente com os riscos enfrentados?
>
> 4. Qual é o impacto na competitividade do Brasil? Se os ataques cibernéticos seguem atingindo bancos, indústrias e infraestrutura crítica, o país pode perder credibilidade internacional e afastar investidores?

2. Cumpre observar, preliminarmente, que é atribuição legal da Secretaria Nacional de Segurança Pública-Senasp do Ministério da Justiça e Segurança Pública (MJSP), conforme estabelecido no Decreto n.º 11.348, de 1º de janeiro de 2023, desempenhar um papel crucial, em diversas áreas, incluindo:

> I - ...
>
> a) na articulação, na proposição, na formulação, na implementação, no acompanhamento e na avaliação de políticas, de estratégias, de planos, de programas e de projetos de segurança pública e defesa social;
>
> c) nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública internacionais, federais, estaduais, municipais e distritais;
>
> II - estimular, propor, promover e coordenar a integração da segurança pública e defesa social no território nacional, em cooperação com os entes federativos, incluídas as organizações governamentais e não governamentais;

3. Concernente à Diretoria de Operações e de Inteligência - DIOPI, esta encontra-se inserida na estrutura organizacional da Secretaria Nacional de Segurança Pública - Senasp, cujas competências estão delineadas no Art. 28 do Decreto nº 11.348, de 2023, nos seguintes termos:

> Art. 28. À Diretoria de Operações Integradas e de Inteligência compete:
>
> I - assessorar a Secretaria nas atividades de inteligência e operações policiais, com foco na integração com os órgãos de segurança pública federais, estaduais, municipais e distritais;
>
> II - implementar, manter e modernizar redes de integração e de sistemas nacionais de inteligência de segurança pública, em conformidade com disposto na Lei nº 13.675, de 2018;
>
> III - promover a integração das atividades de inteligência de segurança pública, em consonância com os órgãos de inteligência federais, estaduais, municipais e distritais que compõem o Subsistema de Inteligência de Segurança Pública;
>
> IV - coordenar o Centro Integrado de Comando e Controle Nacional e promover a integração dos centros integrados de comando e controle regionais;
>
> V - subsidiar o Secretário na definição da política nacional de inteligência de segurança pública quanto à doutrina, à forma de gestão, ao uso dos recursos e às metas de trabalho;
>
> VI - promover, com os órgãos componentes do Sistema Brasileiro de Inteligência, a integração e o compartilhamento de dados e conhecimentos necessários à tomada de decisões administrativas e operacionais por parte da Secretaria; e
>
> VII - propor ações de capacitação relacionadas com a atividade de inteligência de segurança pública, a serem realizadas em parceria com a Diretoria de Ensino e Pesquisa.

4. Neste contexto, é atribuição desta Diretoria o fomento de políticas públicas, com desenvolvimento de projetos e programas, tendo por escopo a inteligência de segurança pública, a integração do Centro Integrado de Comando e Controle Nacional e Estaduais, a proteção das fronteiras e divisas dos estados, dos biomas brasileiros, além do enfrentamento ao crime organizado, tendo por lastro a atuação integrada dos órgãos de segurança pública, nas esferas federal, estadual e municipal, principalmente, por meio das operações integradas.

5. Revela salientar ainda que esta Diretoria de Operações Integradas e de Inteligência **não desenvolve atividades finalísticas de segurança pública, cuja atribuição pertence aos órgãos policiais estaduais e federais, em atenção à autonomia dos entes federados.** Nesse sentido, o que ocorre é a realização de apoio em programas e projetos, por intermédio de demandas dos órgãos solicitantes. Com efeito, a DIOPI desempenha, em verdade, o papel de articulador entre as instituições, fomentando e apoiando a realização de operações integradas preventivas e repressivas a infrações penais, para que os órgãos atuem e se auxiliem mutuamente, dentro de suas atribuições legais, e na medida dos recursos materiais e humanos disponíveis, objetivando atender aos ditames da Lei do Susp (Lei n. 13.675, de 2019).

6. Ademais, como política pública formulada para o enfrentamento ao crime organizado, prevenção da violência e fortalecimento do sistema de segurança pública, além do estímulo à cooperação entre os estados para garantir a proteção dos cidadãos e a manutenção da ordem pública, o Ministério da Justiça e Segurança Pública, por meio da Senasp, no âmbito da DIOPI, mantém o acompanhamento sistemático de temas dentro do escopo que compete à Inteligência de Segurança Pública, em especial sobre eventos que possam gerar impacto na segurança pública, produzindo conhecimento que é compartilhado oportunamente às agências de inteligência federais e estaduais, segundo as regras que regem a atividade de inteligência.

7. Assim, em atenção ao solicitado, apresento as contribuições desta Diretoria aos questionamentos apresentados:

8. O **Laboratório de Operações Cibernéticas**, vinculado à **Diretoria de Operações Integradas e Inteligência (DIOPI)** da **Secretaria Nacional de Segurança Pública (SENASP)**, tem por finalidade apoiar as forças de segurança pública na identificação e combate a ilícitos no ambiente digital. Seu trabalho é pautado na aplicação de inteligência cibernética para **análise de ameaças, suporte a investigações e desenvolvimento de metodologias para o enfrentamento de crimes digitais**.

9. A atuação do laboratório envolve **investigação de ameaças cibernéticas**, na forma de assessoramento técnico às investigações conduzidas pelos órgãos de segurança pública e **identificação de atividades ilícitas no ambiente digital**. Além disso, o Ciberlab colabora com operações integradas e **compartilhamento de boas práticas** para fortalecer a resposta a incidentes cibernéticos.

10. Ao longo de sua atuação, o Ciberlab tem contribuído para **diversas operações de combate a fraudes eletrônicas[1], crimes contra crianças e adolescentes[2], ataques cibernéticos contra infraestruturas críticas[3] e investigações relacionadas a crimes digitais de grande impacto[4]**. Por meio da aplicação de técnicas avançadas de investigação, o laboratório auxilia na **coleta e análise de elementos de informação**, fornecendo suporte para a elucidação de crimes e identificação de redes criminosas que atuam no meio digital.

11. Destacamos também a **Operação Escola Segura**, iniciativa destinada a prevenir e combater ameaças de violência em instituições de ensino. Por meio da atuação contínua de investigação em redes sociais e outras plataformas digitais, o Ciberlab identifica e analisa conteúdos que possam representar riscos às escolas, permitindo a adoção de medidas preventivas e repressivas em colaboração com as forças de segurança estaduais. [5]

12. O laboratório também participa de ações de **capacitação e aprimoramento técnico[6]**, promovendo a especialização de agentes de segurança pública no enfrentamento a crimes cibernéticos. Esse trabalho fortalece a capacidade investigativa das forças policiais e permite a adoção de abordagens mais eficientes na repressão a ilícitos praticados no ambiente digital.

13. Por fim, espera-se ter atendido às questões apresentadas no Requerimento de Informação Parlamentar nº 510/2025, destacando que o Ciberlab/DIOPI/SENASP atua dentro das diretrizes normativas e operacionais estabelecidas, com foco na prevenção, investigação e repressão a crimes cibernéticos. Todas as atividades desenvolvidas pelo laboratório visam fortalecer a capacidade de resposta do Estado diante das ameaças no ambiente digital, garantindo a proteção de infraestruturas críticas, o combate a fraudes eletrônicas e a segurança da sociedade.

14. Colocamo-nos à disposição para quaisquer esclarecimentos adicionais, dentro dos parâmetros legais aplicáveis.

15.

À consideração superior,

PAULO HENRIQUE BENELLI DE AZEVEDO
Coordenador Substituto do Laboratório de Operações Cibernéticas

Ciente. De acordo, encaminhe-se ao Gabinete da Senasp para ciência e providências pertinentes.

RODNEY DA SILVA
Diretor de Operações Integradas e de Inteligência

Documento assinado eletronicamente por **Paulo Henrique Benelli de Azevedo**, **Servidor(a) Mobilizado(a)**, em 06/03/2025, às 11:08, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **RODNEY DA SILVA**, **Diretor(a) de Operações Integradas e de Inteligência**, em 06/03/2025, às 18:31, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

[1] Como por exemplo a Operação Fictus Puella (https://www.gov.br/mj/pt-br/assuntos/noticias/com-o-apoio-do-mjsp-policia-civil-desarticula-organizacao-criminosa-especializada-em-extorsoes-digitais), Operação Falsa Central (https://www.cnnbrasil.com.br/nacional/policia-cumpre-92-mandados-contra-grupo-que-aplicava-golpe-da-falsa-central/) .

[2] Como por exemplo a Operação Bad Vibes, já em sua 3ª fase (https://www.metropoles.com/distrito-federal/na-mira/mjsp-faz-operacao-em-12-estados-contra-exploracao-sexual-infantil).

[3] Como por exemplo a Operação Redirect (https://operacaociber.mj.gov.br/redirect/) e Operação Attack Mestre (https://www.gov.br/mj/pt-br/assuntos/noticias/laboratorio-de-operacoes-ciberneticas-do-ministerio-da-justica-e-seguranca-publica-auxilia-operacao-contra-ataques-virtuais) .

[4] Como por exemplo a Operação 404, já em sua 7ª fase (https://mpsc.mp.br/noticias/gaeco-participa-de-operacao-internacional-contra-a-pirataria) .

[5] https://www.gov.br/mj/pt-br/assuntos/noticias/laboratorio-de-operacoes-ciberneticas-do-mjsp-fortalece-investigacao-sobre-ataques-em-escolas

[6] Como por exemplo os programas Cyber40 https://www.gov.br/mj/pt-br/assuntos/noticias/discord-realiza-treinamento-para-autoridades-policiais-em-evento-organizado-pelo-laboratorio-de-operacoes-ciberneticas-do-ministerio-da-justica-ciberlab

30907541 08027.000148/2025-14

Ministério da Justiça e Segurança Pública
Secretaria Nacional de Segurança Pública

OFÍCIO Nº 2166/2025/GAB-SENASP/SENASP/MJ

Brasília, na data da assinatura.

Ao Senhor
MARIVALDO DE CASTRO PEREIRA
Secretário Nacional de Assuntos Legislativos
Ministério da Justiça e Segurança Pública
Brasília/DF

Assunto: Requerimento de Informação Parlamentar n.º 510/2025, de autoria do Deputado Federal Capitão Alberto Neto (PL/AM).

Senhor Secretário,

1. Cumprimentando-o cordialmente, refiro-me ao Requerimento de Informação Parlamentar n.º 510/2025 (30812652), de 24 de fevereiro do corrente ano, por meio do qual o Deputado Federal Capitão Alberto Neto (PL/AM) requer informações sobre o grande número de ataques cibernéticos no Brasil.

2. Preliminarmente, cabe ressaltar que a competência desta Secretaria Nacional de Segurança Pública é balizada pelo artigo 24 do Decreto n.º 11.348, de 1º de janeiro de 2023, do qual se extrai o papel preponderante na concepção, implementação e avaliação das políticas públicas, com o intuito de fomentar a segurança pública de forma eficaz e eficiente em todo o território nacional, primando pela integração com os entes federativos e norteando-se pelo princípio da autonomia federativa.

3. No escopo dessas atribuições, informo que esta Secretaria dispõe em sua estrutura do Laboratório de Operações Cibernéticas - CiberLab, cuja finalidade é apoiar as forças de segurança pública na identificação e combate a ilícitos no ambiente digital. Para tanto, o CiberLab aplica inteligência cibernética para análise de ameaças, suporte a investigações e desenvolvimento de metodologias para o enfrentamento de crimes digitais. Além de contribuir para operações integradas com esse enfoque, o Ciberlab também promove ações de capacitação e aprimoramento técnico, fomentando a especialização de agentes de segurança pública no enfrentamento a crimes cibernéticos.

4. Por fim, visando contextualizar a atuação desta pasta na temática aduzida pelo parlamentar, encaminho a Informação n.º 29 (30894397).

Atenciosamente,

MARIO LUIZ SARRUBBO
Secretário Nacional de Segurança Pública

Documento assinado eletronicamente por **Mario Luiz Sarrubbo**, **Secretário(a) Nacional de Segurança Pública**, em 10/03/2025, às 20:07, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **30907541** e o código CRC **4632566A**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Anexos:
- Requerimento de Informação Parlamentar n.º 510/2025 (30812652); e
- Informação n.º 29 (30894397).

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 08027.000148/2025-14 SEI nº 30907541

30941109 08027.000148/2025-14

Ministério da Justiça e Segurança Pública
Secretaria Nacional do Consumidor
Gabinete da Secretaria Nacional do Consumidor

OFÍCIO Nº 150/2025/GAB-SENACON/SENACON/MJ

Brasília, na data da assinatura.

Ao Senhor
FRANCISCO FERREIRA
Chefe de Gabinete da Secretaria Nacional de Assuntos Legislativos

Assunto: **Requerimento de Informação Parlamentar** - **RIC nº 510/2025.**

Senhor Chefe de Gabinete,

1. Cumprimentando-o cordialmente, em atenção ao Ofício nº 211/2025/Assessoria-SAL/GAB-SAL/SAL/MJ (30812731), que solicita posicionamento acerca do Requerimento de Informação Parlamentar - RIC nº 510/2025, de autoria do Deputado Capitão Alberto Neto (PL/AM), apresentado à Mesa da Câmara dos Deputados, em 24/02/2025, que "Requer do Ministro da Justiça e Segurança Pública, Senhor Ricardo Lewandowski, informações a respeito do grande número de ataques cibernéticos no Brasil e causaram prejuízo de até R$ 2,3 trilhões na economia brasileira em 2024", encaminho informação nº nº 11/2025/CSA-SENACON/CGCTSA/DPDC/SENACON (30891734) , com manifestações desta Secretaria.

2. Permaneço à disposição para esclarecimentos adicionais.

Atenciosamente,

RICARDO HAACKE SUPPION
Chefe de Gabinete da Secretaria Nacional do Consumidor

Documento assinado eletronicamente por **Ricardo Haacke Suppion**, **Chefe de Gabinete da Secretaria Nacional do Consumidor**, em 11/03/2025, às 16:19, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **30941109** e o código CRC **9BE02279**
O documento pode ser acompanhado pelo site http://sei.consulta.mj.gov.br/ e tem validade de prova de registro de protocolo no Ministério da Justiça e Segurança Pública.

Referência: Caso responda este Ofício, indicar expressamente o Processo nº 08027.000148/2025-14 SEI nº 30941109

REQUERIMENTO DE INFORMAÇÃO Nº DE 2025

(**Do Sr. Capitão Alberto Neto**)

Requer do Ministro da Justiça e Segurança Pública, Senhor Ricardo Lewandowski, informações a respeito do grande número de ataques cibernéticos no Brasil e causaram prejuízo de até R$ 2,3 trilhões na economia brasileira em 2024.

Senhor Presidente,

Com fundamento no art. 50, § 2º, da Constituição Federal, combinado com os arts. 115 e 116 do Regimento Interno da Câmara dos Deputados, requeiro seja encaminhado ao Ministro da Justiça e Segurança Pública pedido de informações a respeito do grande número de ataques cibernéticos no Brasil e causaram prejuízo de até R$ 2,3 trilhões na economia brasileira em 2024.

1) Apesar dos alertas frequentes, quais medidas concretas foram implementadas pelo governo e empresas para fortalecer a segurança digital?
2) Como está a governança da segurança digital no setor público? Grandes órgãos estatais e empresas públicas realmente investem em infraestrutura cibernética ou a proteção digital ainda é negligenciada?
3) O Brasil está investindo em inteligência cibernética à altura da ameaça? Enquanto nações desenvolvidas destinam bilhões para defesa digital, o orçamento brasileiro para segurança cibernética está condizente com os riscos enfrentados?
4) Qual é o impacto na competitividade do Brasil? Se os ataques cibernéticos seguem atingindo bancos, indústrias e infraestrutura crítica, o país pode perder credibilidade internacional e afastar investidores?

Justificativa

Em 2024, o Brasil registrou um número alarmante de ataques cibernéticos, causando prejuízos estimados em R$ 2,3 trilhões para a economia nacional. Esse cenário coloca o país entre os principais alvos globais de crimes digitais, expondo vulnerabilidades tanto no setor público quanto no privado. O crescimento acelerado da digitalização, aliado à fragilidade das infraestruturas de segurança cibernética, tem favorecido a atuação de criminosos que exploram brechas para roubo de dados, fraudes financeiras e ataques contra serviços essenciais.

Diante da magnitude dos danos causados pelos ataques cibernéticos, é dever do governo tomar medidas concretas para fortalecer a segurança digital no país. Segundo o estudo do Instituto Nacional de Combate ao Cibercrime, as Pequenas e Médias Empresas (PMEs) estão mais vulneráveis, por suas limitações financeiras e tecnológicas na adoção de soluções de segurança digital.

O estudo do INCC aponta que cada violação de dados resulta na perda de, em média, 74 empregos e gera um impacto de R$ 26 milhões em massa salarial. No caso das PMEs, as perdas chegam a pouco mais de R$ 2 milhões, eliminando 34 postos de trabalho por ataque.

Sem uma resposta firme e estratégica, o Brasil continuará a ser um terreno fértil para cibercriminosos, sofrendo prejuízos financeiros, instabilidade social e danos à sua reputação global. A segurança digital deve ser tratada como prioridade nacional, e cabe ao governo agir com urgência para proteger a economia e os cidadãos.

Sendo a fiscalização uma das funções típicas do legislador, faz-se necessária a aprovação deste requerimento de informações para obtenção de dados suficientes a respeito da atuação do Poder Executivo, a fim de se assegurar a efetividade das leis ou, se assim for necessário, tomar medidas para que sejam implementadas de forma eficiente e transparente.

Câmara dos Deputados
Gabinete do **Deputado Capitão Alberto Neto** – PL/AM

Termos em que pede deferimento.

Brasília, 24 de fevereiro de 2025.

CAPITÃO ALBERTO NETO
DEPUTADO FEDERAL
PL/AM