COMISSÃO PARLAMENTAR MISTA DE INQUÉRITO DO INSS

(RQN 7/2025)

NORMAS DE FUNCIONAMENTO DA COMISSÃO

O Presidente da Comissão Parlamentar Mista de Inquérito do Instituto Nacional do Seguro Social (CPMI do INSS), criada pelo Requerimento do Congresso Nacional nº 7/2025, com fundamento no art. 89, I, do Regimento Interno do Senado Federal, que confere ao Presidente a competência de organizar e dirigir os trabalhos da Comissão, aplicado nos termos do art. 151 do Regimento Comum do Congresso Nacional, comunica aos membros da Comissão as principais normas regimentais e procedimentais a serem observadas durante os trabalhos:

I – ACESSO AO PLENÁRIO

Art. 1º Consideradas a limitação física do plenário, as disposições contidas no Ato da Comissão Diretora nº 18, de 2014, e as cautelas de segurança para o funcionamento da Comissão, o acesso ao plenário será restrito a apenas:

I. Senadores e Deputados;

II. Três assessores para o Presidente;

III. Cinco assessores para o Relator;

IV. Um assessor para cada membro da Comissão;

V. Um assessor para cada Liderança de Bloco da Câmara dos Deputados e de Bloco do Senado Federal, ou para cada Liderança de Partido não integrante de Bloco, sempre respeitado o disposto no art. 62, §2º, do RISF;

VI. Funcionários da Secretaria-Geral da Mesa do Senado Federal, da Polícia Legislativa do Senado Federal e da Secretaria de Comunicação Social da Câmara dos Deputados e do Senado Federal (imprensa institucional) essenciais ao desempenho das atividades da Comissão;

VII. Cinegrafistas, jornalistas e fotógrafos ligados a outros órgãos de imprensa, autorizados pela Secretaria de Comunicação Social do Senado Federal na forma do art. 3º;

VIII. Consultores legislativos e de orçamento formalmente designados para acompanhar os trabalhos da Comissão;

IX. Advogados formalmente designados para assessorar os trabalhos da Comissão; e

X. Servidores requisitados de outros órgãos em virtude de Requerimento aprovado pela Comissão (art. 89, IX do RISF).

§1º Somente poderão ter entrada e permanência no Plenário pessoas em traje de passeio completo ou vestimenta equivalente, uniforme militar, fardamento profissional ou trajes típicos alusivos à temática da sessão, quando for o caso (Ato da Comissão Diretora nº 14 de 2014).

§2º O acesso ao plenário será controlado por policiais legislativos, que poderão impedir a entrada de quem não estiver autorizado ou descumpra as regras ora fixadas.

Art. 2º A Secretaria de Polícia Legislativa do Senado Federal emitirá crachás de acesso aos servidores especificados no art. 1º.

§1º Os Parlamentares e Lideranças encaminharão e-mail à Secretaria indicando nome, CPF e documento de identificação do servidor responsável por retirar a credencial de acesso perante Secretaria de Polícia Legislativa do Senado Federal.

§2º Os crachás de acesso serão retirados pelo servidor indicado diretamente no Setor de Credenciamento da Secretaria de Polícia Legislativa (SECRED), localizado na garagem coberta do Anexo II, do Senado Federal.

Art. 3º A Secretaria de Comunicação Social do Senado Federal será responsável por controlar o acesso de cinegrafistas, jornalistas e fotógrafos ligados a outros órgãos de imprensa ao plenário em que ocorrerem as reuniões.

Parágrafo único. Se necessário, poderá ser disponibilizado, em plenário distinto, telão para que os demais profissionais possam acompanhar o andamento das reuniões da Comissão.

II - REUNIÕES

Art. 4º As reuniões terão pauta definida pelo Presidente e encaminhada aos membros da Comissão.

Art. 5º Para iniciar a reunião da Comissão é necessária a presença mínima de um terço de sua composição, ou seja, de 11 (onze) parlamentares, considerando-se o total de 32 (trinta e dois) membros (art. 12, RCCN).

Art. 6º Ainda que não haja número para deliberar, poderão ser tomados depoimentos, desde que presentes o Presidente e o Relator (art. 148, § 1º, RISF).

Art. 7º Na hipótese de ausência do Relator a qualquer ato do inquérito, poderá o Presidente da Comissão designar-lhe substituto para a ocasião, mantida a escolha na mesma representação partidária ou bloco parlamentar (art. 147, RISF).

Art. 8º Somente será admitido o uso da palavra como Líder 2 (duas) vezes por reunião: uma pela Liderança do Governo e outra pela Liderança da Oposição, sendo que o Líder necessariamente deverá ser membro.

Parágrafo único. No caso de depoimento, a palavra do Líder será utilizada ao fim da reunião, vedada a interpelação do depoente.

Art. 9º Para o uso da palavra por Líder ou Vice-Líder no exercício da liderança, não é necessário encaminhamento prévio de ofício à Secretaria, mas deverá o parlamentar comunicar à Presidência qual liderança exerce, certificando-se de não estarem presentes em plenário o respectivo Líder ou Vice-Líder com precedência.

Art. 10. É assegurado o uso da palavra "pela ordem", para indagação a respeito do andamento dos trabalhos ou reclamação quanto à observância dos regimentos, por 5 (cinco) minutos (art. 14, X, RISF).

Art. 11. É assegurado o uso da palavra para suscitar questão de ordem sempre que houver dúvida sobre a interpretação regimental, na sua prática exclusiva ou relacionada à Constituição, por 5 (cinco) minutos (art. 131, RCCN).

III - REQUERIMENTOS

Art. 12. Os Requerimentos poderão ser apresentados apenas pelos membros da Comissão, por meio do sistema eletrônico de cada Casa: LexEdit e Infoleg Autenticador, para a Câmara dos Deputados, LexEdit e Sedol, para o Senado Federal.

Art. 13. Os Requerimentos de convocação deverão ser individualizados e identificar com precisão a pessoa a que se dirigem por seu nome e qualificação.

Parágrafo único. Os Requerimentos com múltiplos convocados ou com identificação genérica poderão ser recusados.

Art. 14. No caso de múltiplos Requerimentos de convocação ou convite para o depoimento de uma mesma pessoa, será apreciado com precedência aquele de autoria do Relator ou indicado pelo Presidente.

Parágrafo único. Havendo a aprovação ou rejeição de Requerimento de convocação ou convite, os demais Requerimentos sobre o mesmo tema serão considerados aprovados exclusivamente para fins precedência na interpelação ao depoente de que trata o art. 27, II.

Art. 15. Os Requerimentos de transferência de sigilo bancário, fiscal ou telefônico deverão conter, além da fundamentação adequada (motivação específica, pertinência temática com a investigação e necessidade absoluta da medida), a identificação inequívoca do alvo, mediante a indicação do nome completo e do CPF ou do CNPJ, e o período referente à transferência.

Parágrafo único. Cada Requerimento deverá fazer referência exclusivamente a um único alvo.

Art. 16. Os Requerimentos de transferência de sigilo telemático, além de conter fundamentação adequada, deverão ser formulados com identificadores válidos que possibilitem o seu cumprimento, especificar os dados a serem obtidos a partir de sua aprovação e o período referente à transferência.

Art. 17. Como parâmetro para a elaboração dos Requerimentos de transferência de sigilo telemático, os parlamentares poderão se valer, além das informações prestadas pelas respectivas plataformas de tecnologia às autoridades de persecução criminal, do relatório elaborado pela Coordenação de Comissões Especiais Temporárias e Parlamentares de Inquérito a partir de consulta formulada às principais plataformas, que constitui o Anexo I destas Normas de Funcionamento.

Art. 18. Os Requerimentos que tratem de busca e apreensão deverão ser apresentados Secretaria sigilosamente, em envelope lacrado, conter fundamentação idônea e informações inequívocas sobre o objeto da medida.

Art. 19. O Requerimento apresentado à Comissão que não estiver de acordo com as orientações especificadas acima poderá ser recusado pela Secretaria e não será submetido à deliberação da Comissão, entretanto seu autor poderá reapresentá-lo, após o devido saneamento.

Art. 20. Os Requerimentos não admitirão discussão, podendo eventualmente ter sua votação encaminhada por 2 (dois) membros de cada Casa, de preferência um favorável e um contrário, pelo prazo de até 5 (cinco) minutos (art. 41, RCCN).

Art. 21. A Comissão, com paridade entre Senadores e Deputados, deliberará por maioria de votos, presente a maioria de seus membros, considerando-se o conjunto dos integrantes da Comissão, e o Presidente somente terá o voto de desempate (art. 14, parágrafo único, RCCN).

Art. 22. O Requerimento de verificação de votação só será admitido se formulado por líder, 5 (cinco) Senadores ou 20 (vinte) Deputados (art. 45, § 1º, RCCN).

IV - USO DA PALAVRA EM OITIVAS

Art. 23. As listas de inscrição serão disponibilizadas para assinatura exclusivamente no plenário em que será realizada a reunião da Comissão, com antecedência de 30 (trinta) minutos do horário marcado para seu início.

Parágrafo único. Para a assinatura da lista de inscrição, os parlamentares deverão se dirigir pessoalmente ao plenário, vedada a assinatura por procuração ou assemelhada.

Art. 24. As inscrições serão obrigatoriamente encerradas após 1 (uma) hora da abertura da reunião.

Art. 25. Nos depoimentos e inquirições, o Presidente franqueará inicialmente a palavra ao depoente por 15 (quinze) minutos, prorrogáveis por, no máximo, 5 (cinco) minutos.

Art. 26. A seguir, o Relator interpelará o depoente pelo prazo que for necessário.

Art. 27. Após o Relator, os questionamentos seguirão a seguinte ordem:

I. o autor do Requerimento aprovado de convocação ou convite mais antigo que estiver presente;

II. os titulares, na ordem da respectiva inscrição;

III. os suplentes, na ordem da respectiva inscrição; e

IV. os não-membros, na ordem da respectiva inscrição (art. 112, RISF).

Parágrafo único. Os membros disporão do prazo para as interpelações de até 10 (dez) minutos e os não-membros de até 3 (três) minutos.

Art. 28. O Presidente e o Relator poderão interpelar o depoente ou prestar esclarecimentos a qualquer instante do depoimento.

Art. 29. O Presidente deverá alertar o interpelante sobre pergunta que já houver sido respondida pelo depoente, a fim de se evitar repetições desnecessárias.

Art. 30. Antes do encerramento da oitiva, o Presidente poderá franquear a palavra ao depoente por até 5 (cinco) minutos para suas manifestações finais.

Art. 31. Caso o membro, autorizado pelo Presidente, use recursos audiovisuais em suas interpelações, firmará previamente Termo de Compromisso por meio do qual assume integral responsabilidade pessoal, independentemente de dolo ou culpa, pela transmissão do conteúdo, eximindo totalmente de responsabilidade qualquer terceiro, inclusive o Presidente, a Secretaria, a mídia institucional, a Comissão ou quaisquer dos demais membros por eventuais violações e repercussões delas decorrentes, inclusive se forem de conteúdo econômico.

§1º O membro obriga-se a encaminhar, pessoalmente ou por meio de sua assessoria, à Secretaria, mídias que não representem qualquer violação à Lei, compreendida em seu sentido mais amplo, incluindo, mas não se limitando a direitos autorais, hipóteses de sigilo legal ou de segredo de justiça, segredo de indústria, direitos de propriedade intelectual e industrial, a dados pessoais, ou à honra e à imagem de terceiros.

§2º Sem prejuízo da responsabilidade pessoal e exclusiva do membro, este reconhecerá e aceitará que, se for possível a análise prévia do material, a Secretaria e a Presidência poderão, a seu exclusivo critério, impedir ou interromper a exibição de conteúdo que compreendam potencialmente violador da Lei, compreendida em seu sentido mais amplo.

V – INVESTIGAÇÕES E ACESSO À DOCUMENTAÇÃO SIGILOSA

Art. 32. Os documentos serão recebidos pela Comissão e serão classificados pela Secretaria de acordo com as hipóteses legais de sigilo.

Art. 33. Os membros da Comissão poderão se cadastrar para acessar a documentação sigilosa.

Parágrafo único. O acesso a documento de natureza sigilosa poderá ser realizado, no exercício de suas atribuições funcionais estritamente vinculadas ao inquérito parlamentar e tão somente na medida necessária, por:

I. Servidores da Secretaria de Comissão, com o objetivo de cadastrar e organizar a documentação recebida;

II. Consultores Legislativos ou Consultores de Orçamentos formalmente designados pelo respectivo Consultor-Geral, a pedido do Presidente da Comissão, para o acompanhamento das investigações e das análises empreendidas pela Comissão ou por membro;

III. Advogados do Senado, formalmente designados pelo Advogado-Geral, a pedido do Presidente da Comissão, para a elaboração de manifestações em processos de natureza judicial ou extrajudicial, de estudos e de pareceres jurídicos que forem necessários;

IV. Servidores da área de informática legislativa, designados, a pedido do Presidente da Comissão, pelo Diretor da Secretaria de Informática Legislativa, com vistas a implementar correções e modificações nos sistemas que, eventualmente, exijam acesso à base de dados de documentos sigilosos.

V. Policiais Legislativos formalmente designados pelo Diretor de Polícia Legislativa, a pedido do Presidente da Comissão, para o acompanhamento das investigações e das análises empreendidas pela Comissão ou por membro;

VI. Servidores de outros órgãos requisitados para atendimento à Comissão, para a condução das investigações e das análises necessárias à Comissão ou a membro; e

VII. Servidores lotados no gabinete de membro da Comissão, os quais acessarão os documentos sob responsabilidade exclusiva do membro que os houver indicado, para o acompanhamento das investigações e das análises empreendidas pela Comissão ou por membro da Comissão.

Art. 34. O acesso a documento de natureza sigilosa realizado pelas pessoas indicadas nos incisos II, III, IV e V do parágrafo único do art. 33 será limitado a 4 (quatro) servidores, designados em ato formal pelo titular do órgão.

Art. 35. Em linha com a prática aplicável a outras comissões, cada membro poderá indicar, na forma do art. 33, parágrafo único, inciso VII, 1 (um) assessor para acesso à documentação sigilosa, informando o seu nome completo, matrícula e CPF, por meio de ofício endereçado ao Presidente, a ser protocolizado por meio do Infoleg Autenticador, para Deputados, e Sedol, para Senadores.

Parágrafo único. O Presidente poderá indicar até 3 (três) assessores, e o Relator até 4 (quatro), para acesso aos documentos sigilosos.

Art. 36. O acesso a documentos sigilosos por parlamentares, seus assessores e demais servidores seguirá as seguintes diretrizes:

I. Deverá ser preenchido e assinado um Termo de Confidencialidade e Sigilo no momento do cadastro para acesso à documentação sigilosa;

II. O acesso à documentação sigilosa será feito por meio eletrônico, em sistemas próprios do Senado Federal para acesso de documentos de CPIs, que mantenham o registro dos acessos realizados (Drive Jubarte, Sittel e Simba); e

III. O cadastro para acesso aos documentos sigilosos deverá ser realizado junto à Secretaria da Comissão.

Parágrafo único. O Presidente restringirá o acesso ao Sittel e ao Simba a servidores especificamente designados para tal finalidade, a partir de pedido fundamentado formulado pelo Relator ou por membro.

Art. 37. O Presidente poderá adotar critérios ainda mais rigorosos para o acesso a documentos sigilosos específicos, inclusive limitando quais membros e servidores farão jus ao referenciado acesso, bem como se valendo do uso de Sala de Documentos.

Art. 38. A Sala de Documentos, destinada a documentos cujo acesso não se dará por meio dos sistemas, compreenderá, seguindo as diretrizes de segurança traçadas pelo Prodasen, pela SPOL e pela Comissão, computadores ou documentos impressos para acesso por servidor ou membro da Comissão devidamente autorizados, respeitadas as seguintes diretivas:

I. Aparelhos de telefone celular e demais dispositivos informáticos serão deixados fora da Sala de Documentos;

II. Os servidores ou parlamentares credenciados deverão permanecer na Sala de Documentos somente pelo tempo necessário para a análise dos documentos que lá se encontrem, podendo tão somente tomar notas, vedada a utilização de câmeras, pen drive ou de qualquer dispositivo que permita o registro dos documentos acessados;

III. Antes de sair da Sala de Documentos, o credenciado preencherá de forma manuscrita o Livro de Registro de Acessos, com as seguintes informações relativamente ao acesso efetuado: nome, dia, hora de entrada e saída, motivo do acesso e assinatura; e

IV. Os servidores da COCETI poderão acompanhar, parcial ou integralmente, o acesso do servidor ou do membro da Comissão à Sala de Documentos, bem como poderão contar com o auxílio da SPOL para esse fim, inclusive com uso de detector de metais e monitoramento presencial, se necessário for.

Art. 39. No acesso à documentação sigilosa, a pessoa autorizada deverá adotar todas as cautelas para resguardo do sigilo, manter em segurança as suas senhas, códigos de acesso e dados pessoais para acesso aos sistemas informáticos, atentando-se à sua pessoalidade e à sua intransferibilidade em relação a quaisquer terceiros, bem como diligenciar para que, durante a sua ausência, o computador esteja com a tela manualmente bloqueada, de modo a impedir qualquer forma de acesso indevido por terceiros.

Art. 40. No caso de quebra do sigilo das informações, devidamente comprovada, o responsável estará sujeito, por ação ou omissão, às sanções cabíveis, apuradas na forma da lei.

Brasília, 26 de agosto de 2025.

SENADOR CARLOS VIANA

Presidente da CPMI do INSS

ANEXO I - TRANSFERÊNCIAS DE SIGILO TELEMÁTICO

Informações coletadas junto às plataformas de tecnologia em 2023 pela Coordenação de Comissões Especiais, Temporárias e Parlamentares de Inquérito para auxiliar os gabinetes parlamentares na elaboração de Requerimentos de transferência de sigilo telemático:

- **Instagram (META)**
    - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):
        - URL
        - Alias (ex.: @nome)

    - Dados que poderiam ser requisitados pela Comissão
        - Dados cadastrais
        - Localização
        - Mensagens
        - Comentários
        - Curtidas

- **Facebook (META)**
    - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):
        - endereço URL, tal como https://www.facebook.com/profile.php?id=000000000000000
        - número de telefone (incluindo +55 se o terminal for do Brasil ou o código de área do país de origem)
        - endereço de e-mail.

    - Dados que poderiam ser requisitados pela Comissão
        - Dados cadastrais do usuário, incluindo nome completo, endereço, telefone e e-mail
        - Logs de acesso, com IP, data, hora e horário GMT/UTC
        - Conteúdo de mensagens, posts, fotografias e vídeo

- **WhatsApp (META)**
    - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):
        - Número de telefone (formato +código de país, código de área, número)
        - ID do Grupo, caso possuir

- Dados que poderiam ser requisitados pela Comissão
  - Número do terminal telefônico
  - Nome do usuário
  - Modelo do Aparelho
  - Versão do Aplicativo
  - Data inicial e final
  - Status da conexão
  - Data da última conexão
  - Endereço de e-mail
  - Informações do cliente WEB
  - Informações dos grupos de que participa, incluindo data de criação, descrição, identificador de grupo (Group ID), foto, quantidade de membros, nome do grupo e participantes.
  - Mudanças de números
  - Contatos (incluindo contatos em que o alvo tem o número do contato em sua agenda e o contato tem o número do alvo na sua, e aqueles em que apenas um dos dois possui registro na agenda)
  - Foto do perfil
  - Status antigos
  - Registro de IP
  - Histórico de chamadas efetuadas e recebidas

- **Google (GOOGLE LLC e Partes Relacionadas)**
  - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):
    - E-mail Google: XXXX@gmail.com

  - Dados que poderiam ser requisitados pela Comissão: dados relativos a qualquer *produto google*
    - Dados cadastrais
    - Registros de conexão (IPs)
    - Informações de Android (IMEI)
    - Conteúdo de Gmail
    - Conteúdo de Google Fotos, com os respectivos metadados (EXIF)
    - Conteúdo de Google Drive
    - Lista de contatos
    - Histórico de Localização
    - Histórico de Pesquisa
    - Histórico de Navegação
    - Conteúdo de Waze

- Logs de acesso com IP/Data/Hora/ e fuso horário de criação e acesso em determinado período de tempo de contas de Gmail;
- Logs de acesso com IP/Data/Hora/ e fuso horário de criação e acesso em determinado período de tempo em canal do YOUTUBE especificado por meio da URL do vídeo ou do canal;
- Logs de acesso com IP/Data/Hora/ e fuso horário de acesso para a veiculação de vídeo veiculado no YOUTUBE especificado por meio da URL do vídeo ou do canal;
- Dados armazenados na "Sua linha de tempo" do Google Maps e outras informações de localização;
- Histórico de exibição, histórico de pesquisas, curtidas e comentários do Youtube;
- Histórico de pesquisas no Google Pesquisa (termos pesquisados);
- Imagens armazenadas no Google Fotos;
- Dados armazenados no Google Drive, incluindo backup do WhatsApp e de outros aplicativos de comunicação que realizem backup por intermédio do Google;
- Caixa de entrada, enviados, rascunhos e lixeira do Gmail, bem como dados cadastrais, registros de acessos, contendo data, horário, padrão de fuso horário e endereçamento IP;
- Histórico de navegação do Google Chrome sincronizados com a conta do Google;
- Lista de contatos;
- Informações sobre tipo e configurações de navegador, tipo e configurações de dispositivo, sistema operacional, rede móvel, bem como interação de apps, navegadores e dispositivos com os serviços do Google;
- Informações sobre aplicativos adquiridos e instalados por meio da PlayStore;
- Caso o alvo utilize os serviços do Google para fazer e receber chamadas ou enviar e receber mensagens, a empresa deve apresentar as informações que possuir;
- Informações de voz e áudio caso o alvo utilizar recursos de áudio;
- Pessoas com quem o alvo se comunicou e/ou compartilhou conteúdo;
- "Históricos de alteração de conta" e os respectivos e-mails anteriores para recuperação de conta

- **Telegram**
  - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):

- Número de telefone (formato +código de país, código de área, número)

- Dados que poderiam ser requisitados pela Comissão: não foi informado

- **Apple**
  - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):
    - Número de série (SN)
    - IMEI (O código International Mobile Equipment Identity é um código numérico único e global presente em aparelhos que se conectam às redes celulares, como smartphones, tablets e modems 4G ou 5G.)
    - MEID (O Mobile Equipment Identifier é um código de identificação global de dispositivos móveis que atuam em redes de internet móvel CDMA (tecnologia relacionada ao 3G). Criado em 2006, o "registro" substitui o número de série eletrônicos (ESN), cujas combinações se esgotaram em novembro de 2008.)
    - MAC ADDRESS
    - TELEFONE CELULAR + IDENTIFICAÇÃO DO ALVO
    - GUID
    - Apple ID
    - DSID (O Directory Services Identifier é um método para identificar contas AppleID. É o equivalente ao número serial de equipamentos, aqui associado a uma conta AppleID ou iCloud para uso na identificação de casos no iLog, a ferramenta de suporte do iCloud, ou para verificar um cliente na linha)
    - Nome completo e número de telefone e endereço físico.

  - Dados que poderiam ser requisitados pela Comissão
    - Registro de dispositivos, incluindo nome, e-mail, endereço e telefone (fornecidos pelo usuário);
    - Registro de atendimento ao cliente pela Apple;
    - Dados do iTunes, incluindo nome, endereço físico, endereço de e-mail e número de telefone (fornecidos pelo usuário), conexões e transações de compra/download do iTunes, conexões de atualização/novo download e registro de conexões e informações do assinante iTunes, com endereços IP
    - Compras em lojas físicas (mediante número do cartão de crédito) e compras em lojas online (mediante número do cartão de crédito ou Apple ID) - informam, inclusive, o endereço físico da entrega;
    - Informações de backup de aparelhos;

- Dados cadastrais do iCloud, incluindo nome completo, endereço, telefone e email (fornecidos pelo usuário);
- Logs de acesso, com IP, data, hora e horário GMT/UTC;
- Conteúdo do iCloud, incluindo fotos, vídeos, mensagens SMS, MMS ou iMessage, e correio de voz, documentos, contatos, calendários, favoritos, histórico de navegação do Safari, e backup de dispositivos iOS

- **Twitter**
  - Identificador válido (indicar no Requerimento pelo menos um destes identificadores):
    - Nome do usuário (com o signo "@")
    - identificador URL
  - Dados que poderiam ser requisitados pela Comissão
    - Nome, sobrenome, senha, email e nome de usuário
    - Localização, foto da conta e do fundo
    - Número de celular para recebimento de SMS e catálogo de endereços
    - Tweets, as contas seguidas, tweets favoritos
    - Coordenadas exatas da localização dos tweets
    - Endereços IPs, data/hora/fuso
    - Navegador utilizado
    - Domínio referente
    - Páginas visitadas
    - Operadora do dispositivo móvel
    - IDs de aplicativos e termos de buscas
    - Links visitados e quantidade de vezes que foi clicado.