INSTITUTO FEDERAL DE SANTA CATARINA

JÉSSICA DA SILVA HAHN

Interceptação legal em centrais telefônicas IP

São José - SC

julho/2019

INTERCEPTAÇÃO LEGAL EM CENTRAIS TELEFÔNICAS IP

Pré-Projeto de trabalho de conclusão de curso apresentado à Coordenadoria do Curso de Engenharia de Telecomunicações do campus São José do Instituto Federal de Santa Catarina para a aprovação do tema perante banca na disciplina de TCC1.

Orientador: Jorge Henrique Busatto Casagrande

Coorientador: Ederson Torresini

São José - SC

julho/2019

RESUMO

A demanda cada vez maior na investigação judicial de chamadas telefônicas dentro do crescente tráfego nas redes das operadoras, incluindo aquelas com tecnologia *Voice Over Internet Protocol* (VoIP), implicou na necessidade do provisionamento de técnicas padronizadas para a captura legal de informação dessas chamadas. Uma operadora tem a obrigação legal de realizar uma interceptação telefônica e disponibilizar os dados capturados a uma autoridade policial se assim for solicitado. Entretanto o processo de interceptação não é uma tarefa simples e envolve um conjunto de fatores tais como legislações e tecnologias de acesso correspondentes. Realizar várias interceptações simultaneamente é um desafio para os provedores desse serviço, pois envolve muitos procedimentos incluindo a configuração manual dos equipamentos nos nós das redes. Dado essas circunstâncias, o objetivo deste trabalho é possibilitar a implementação de um serviço de interceptação usando um cenário de testes que utilize a tecnologia VoIP, usando preferencialmente ferramentas *open source* e respeitando os modelos descritos nas normas internacionais e a legislação brasileira. Serão realizados os seguintes procedimentos: estudo e aplicabilidade das tecnologias e padrões de automatização; estudo e aplicabilidade dos principais equipamentos VoIP; definição e implantação de um modelo de interceptação descritos nas normas, como as normas *European Telecommunications Standards Institute* (ETSI) e, como meta maior, a implementação de automatização de uma interceptação entre dois *User Agent* (UA)s tal como em um cenário real.

Palavras-chave: Interceptação legal. ETSI. VoIP.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

PSTN *Public Switched Telephone Network* 19

MGC *Media Gateway Controller* 19

IP PBX *Internet Protocol Private Branch Exchange* 34

SR *Sender Report* 30

RR *Receiver Report* 30

ABNT *Associação Brasileira de Normas Técnicas* 17

SFTP *SSH File Transfer Protocol* 23

RNP *Rede Nacional de Ensino e Pesquisa* 34

SUMÁRIO

1 INTRODUÇÃO

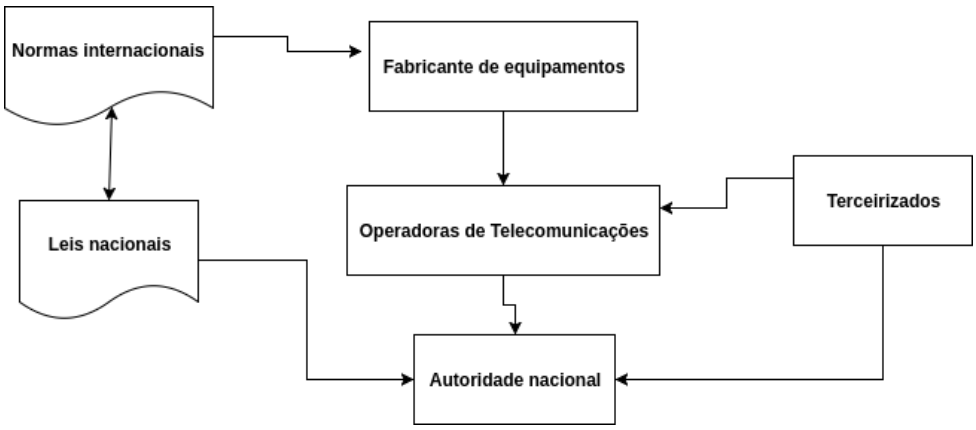
Os avanços tecnológicos permitiram o surgimento de celulares. Com o passar do tempo eles ganharam poder de processamento, permitindo criar aplicativos com inúmeras funcionalidades, como por exemplo, aplicativos que transmitem voz pela internet e dados de navegação em portais web. Proporcionalmente houve um grande crescimento do número de usuários e da quantidade de tráfego de dados nas operadoras de telefonia. Em 2019 o Brasil registrou 228.633.074 milhões de acessos a serviços pessoais móveis, sendo mais de 135 milhões de acessos através da tecnologia 4G (ANATEL, 2019).

Do ponto de vista legal uma operadora tem a obrigação de entregar dados de navegação e as ligações realizadas por seus clientes que estão sob investigação criminal. Conforme descrito na lei Nº 9.296/1996 que rege a interceptação telefônica no Brasil. Além disso uma operadora tem a obrigação legal de realizar uma interceptação telefônica e disponibilizar os dados capturados a uma autoridade policial se assim for solicitado.

Em função do que é previsto em lei, surge os termos de interceptação legal e quebra de sigilo de dados. Cada país determina como esses processos devem ser realizados. Nesse contexto, em 1995 esse tema ganhou grande relevância pelo *European Telecommunications Standards Institute* (ETSI), organização europeia responsável por padronizar serviços de telecomunicações, radiofusão e outras comunicações eletrônicas. Ademais essa organização passou a normatizar a interceptação legal pelo continente europeu (ETSI, 2019a).

Executar uma interceptação legal não é uma tarefa simples, pois os seguintes fatores influenciam o desenvolvimento de um serviço de interceptação: os equipamentos de telecomunicações, as operadoras, as normas internacionais, a legislação de um país, as forças de segurança nacional e por fim, empresas terceirizadas que podem atuar na interceptação. Os fabricantes baseiam-se em normas internacionais para produzirem os equipamentos. Os provedores dependem deles para montar sua rede. E devem obedecer a legislação e autoridade nacional (ETSI, 2006b). A Figura 1 apresenta os envolvidos nesse processo.

Figura 1 – Fatores que influenciam a implementação de serviços de interceptação legal.



Fonte: Adaptado de (ETSI, 2006b).

1.1 Justificativa

A interceptação telemática nas redes das operadoras torna-se cada vez mais complicada, devido a complexidade da rede de telefonia. Pela existência dos diversos padrões e tecnologias, como por exemplo, *IP Multimedia Core Network Subsystem* (IMS), 3G e 4G, presentes na telefonia móvel. A própria norma brasileira não estabelece um modelo de serviço de interceptação dentro da rede dos provedores. A norma apenas recomenda utilizar um formato e protocolo específico para a entrega dos dados coletados. Logo a operadora pode realizar esse processo de forma independente. Entretanto, implementar centenas de interceptações em um mesmo período de tempo é um grande problema, pois configurar isso manualmente levaria muito tempo. Automatizar esse processo portanto, é essencial. Em adição, há questões técnicas, de mercado, entre outros fatores que definem a adoção de fabricante ou tecnologia para implementar esse serviço. E isso torna o cenário de interceptação mais complexo ainda.

Em uma pesquisa preliminar, não foi encontrado nenhuma ferramenta de baixo custo que auxilie no provisionamento de uma interceptação legal. Por outro lado, há limitações de tempo, restrições de uso da rede do IFSC, dentre outras questões técnicas que levam a restringir o escopo deste trabalho. No entanto, o tema é atual e envolvente com o crescente uso da tecnologia VoIP dentro da diversidade da rede de telefonia. Propor uma automatização na interceptação de uma conversa telefônica, dentro de um cenário controlado usando procedimentos padrão e legais, é um passo motivador para se abrir uma janela de oportunidades de outros trabalhos nesta área.

1.2 Objetivo geral

Apresentar uma solução de baixo custo para automatização de interceptações legais em centrais telefônicas IP.

1.3 Objetivos específicos

- Avaliar os padrões e tecnologias de automatização, preferencialmente *open source*, para configuração de sistemas computacionais.
- Identificar como os equipamentos comerciais realizam o processo de interceptação.
- Implementar um cenário de interceptação utilizando a tecnologia VoIP.
- Realizar a interceptação e o desvio de ligações VoIP de um usuário e armazená-las em um servidor.

No segundo capítulo a seguir serão abordados os seguintes temas: a legislação brasileira sobre interceptação e quebra de sigilo de dados, assim como a diferença entre esses dois termos. Será descrito as normas internacionais e a norma brasileira que definem padrões de interceptação legal, a tecnologia VoIP e por fim a complexidade da implementação de cenários de interceptação segundo as normas. No terceiro capítulo é discutido como será a proposta do trabalho e a estratégia metodológica pretendida para a realização deste estudo.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Diferenças entre interceptação legal e quebra de sigilo

Em um processo judicial pode ser necessário a aplicação de meios tecnológicos para obtenção de provas. A lei Nº 9.296 explicita que a interceptação legal e a quebra de sigilo pode ser utilizada como prova de investigação criminal. As seções a seguir apresentam uma pequena definição para esses termos, com base no estudo realizado.

2.1.1 Interceptação legal

É o ato de apoderar-se de algo antes que alcance o respectivo destinatário (GUARDIA, 2012), também conhecida pelo termo em inglês *Lawful Interception* (LI). Já no âmbito das telecomunicações, a interceptação legal refere-se ao acesso sancionado por lei a comunicações privadas, no qual um provedor de serviço de telecomunicações coleta e fornece às autoridades policiais, comunicações interceptadas de indivíduos, instituições privadas ou organizações públicas (ETSI, 1995).

Conforme as definições acima e segundo a lei brasileira Nº 9.296, onde uma interceptação possui um prazo determinado de quinze dias a partir da data do ofício judicial. Determina-se que uma interceptação legal é o ato de utilizar meios técnicos para coletar dados telemáticos que estão em fluxo a partir de um período temporal.

2.1.2 Quebra de sigilo

Segundo GUARDIA (2012), o projeto de lei Nº 3.272/2008 define a quebra de sigilo das comunicações telefônicas de qualquer natureza todo ato que intervém o fluxo dessas comunicações, com a finalidade de obter conhecimento das informações transmitidas. Conclui-se que uma quebra de sigilo é um termo geral utilizado para referenciar o ato de por fim ao sigilo (segredo) de qualquer informação coletada. E a interceptação é um dos meios de obter esses dados.

2.2 Legislação brasileira

Por se tratar de um tema de soberania nacional, cada país determina leis que regem a interceptação telefônica juntamente com a quebra de sigilo desses dados. Nas seções a seguir serão apresentadas algumas leis que relatam as obrigações das operadoras em termos de coleta, disponibilização e proteção dos dados.

2.2.1 Constituição federal

A constituição brasileira de 1988, artigo 5º, inciso XII (BRASIL, 1988), prevê que todo e qualquer cidadão tem por direito que suas comunicações de dados e telefônicas sejam mantidas sob sigilo, sendo que sua violação só será possível mediante ordem judicial, para fins de investigação criminal. Por prever apenas o sigilo das comunicações houve a necessidade de regulamentar as interceptações telefônicas. A lei Nº 9.296/1996 e Nº 12.965/2014 em conjunto com a resolução Nº 59 abordam esse tema.

2.2.2 Interceptação telefônica

A lei Nº 9.296 descreve explicitamente as interceptações telefônicas, abrangendo sistemas de informática e telemática (BRASIL, 1996). Segundo ela a interrupção do fluxo de comunicação só será

realizada mediante ofício, ou requerimento, aprovado judicialmente (Art. 3º). O alvo em questão terá que estar sob investigação criminal e não havendo outro meio de obtenção de prova a interceptação poderá ser realizada (Art. 1º e Art. 2, inciso II).

A interceptação não poderá exceder o prazo de quinze dias, após esse período deverá ser interrompida, podendo ser renovada somente mediante a um novo ofício (Art. 5º). Qualquer interceptação sem ordem judicial é crime com pena de reclusão de dois a quatro anos e multa (Art. 10º).

As informações coletadas poderão ser gravadas, conforme diligência (ato judicial). Sendo transcritas obrigatoriamente e entregues a autoridade policial que encaminhará ao juiz responsável pela investigação (Art. 6º , parágrafo 1º e parágrafo 2). Todas as informações interceptadas, assim como os dados referentes ao processo de investigação, deverão ter o sigilo preservado (Art. 8º). Ou seja, somente pessoas autorizadas terão acesso a essas informações.

Um provedor só interceptará o seu assinante e todos os dados coletados, inclusive informações de outros usuários, que se comunicam com esse alvo. Essas interceptações serão entregues a autoridade para posterior análise.

2.2.3 Marco Civil da internet

Lei Nº 12.965/2014 estabelece os direitos e deveres para o uso dos serviços de internet no Brasil (BRASIL, 2014). O provedor será obrigado a apresentar a uma autoridade, mediante ordem judicial, os registros de conexões e de acesso a aplicações de internet, os dados pessoais, o conteúdo das comunicações privadas, ou outras informações que possibilitem a identificação do usuário ou do seu terminal de acesso. (Art. 10, parágrafo 1º).

Os registros de conexões deverão ser mantidos em sigilo, em ambiente seguro por um período de um ano (Art. 13). Os registros de acesso a aplicações de internet deverão ser guardados apenas por seis meses (Art. 15).

A requisição judicial para acesso aos registros deverá conter informações da investigação que fundamente o acesso ao histórico do investigado, assim como os indícios da ocorrência. E principalmente o período no qual se referem esses registros (Art. 22, incisos I, II e III).

A lei define um registro de conexão como o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal. Por fim a lei descreve que os registros de acesso a aplicações de internet são as informações referentes à data e hora de uso de uma determinada aplicação a partir de um determinado endereço IP (Art. 5º, incisos V, VI e VIII).

A lei do Marco Civil até a presente data da entrega deste trabalho não está em vigor em nosso país.

2.2.4 Resolução Nº 59 de 09 de setembro de 2008

De acordo com (CNJ, 2008) o ofício contendo o pedido de interceptação entregue as operadoras deverá conter principalmente :

- O número do telefone, e-mail, ou outro identificador do alvo a ser interceptado.
- O número do ofício.
- Data da distribuição.

- Número do inquérito ou processo.
- Identificação do órgão que solicitou a interceptação.
- A expressa vedação de interceptação de outros números não discriminados na decisão.

2.3 Normas internacionais

Durante a pesquisa documental constatou-se que há dois órgãos internacionais relevantes para o trabalho. O padrão europeu *European Telecommunications Standards Institute* (ETSI) que é citado pela *Associação Brasileira de Normas Técnicas* (ABNT) na norma ABNT-NBR 16386:2015. E o padrão americano está definido pela CALEA, cuja tradução é Lei de Auxílio das Comunicações para a Aplicação do Direito.

2.3.1 O padrão europeu ETSI

O *European Telecommunications Standards Institute* é responsável por criar normas para os serviços de telecomunicações. Apesar de inicialmente ter sido criada apenas para atender o mercado europeu, atualmente é constituída por mais de oitocentos e cinquenta organizações ao redor do mundo. Inclusive por grandes empresas, como mostra a Tabela 1.

Tabela 1 – Principais membros ETSI

Membros	**Atuação**	**País**
Amazon	Comércio eletrônico, serviços em nuvem	Estados Unidos
Bluetooth SIG Inc.	Grupo responsável por padronizar e fiscalizar os padrões da tecnologia bluetooth	Estados Unidos
Broadcom Corporation	Fabricante de semicondutores e eletrônicos	Estados Unidos
Juniper Networks	Fabricante de equipamentos de rede	Estados Unidos
Oracle Corporation	Atua no comércio de produtos de hardware e software	Estados Unidos
Wi-Fi Alliance	Responsável pela criação da tecnologia Wi-fi	Estados Unidos
Huawei Technologies	Fabricante de equipamentos de rede	China
Cisco Systems	Fabricante de equipamentos de rede	Bélgica e França

Fonte: (ETSI, 2019b)

O ETSI é responsável por publicar especificações técnicas de interceptação de dados telemáticos. Foram selecionados alguns padrões relevantes para o escopo deste trabalho, sendo os principais:

- Padrão ETSI TR 101 943 : aborda os conceitos gerais para interceptação em um rede genérica (ETSI, 2006b).
- Padrão ETSI TR 102 528: especifica uma arquitetura genérica para uma rede IP (ETSI, 2006a).
- Padrão ETSI TS 102 232-5: especifica a interceptação para serviços de multimídia IP (ETSI, 2019c).

2.3.1.1 Padrão ETSI TR 101 943

Essa norma define um padrão geral de arquitetura para a implementação de um serviço de interceptação onde há cinco atores principais representados na Figura 2. Na qual pode-se descrevê-los da seguinte forma:

- *Law Enforcement Agency* (LEA): autoridade nacional que faz a requisição das interceptações e recebe os dados coletados.

- *Law Enforcement Monitoring Facility* (LEMF): aplicação que irá receber os resultados da interceptação.
- *Internal Intercepting Function* (IIF): ponto dentro de uma rede em que o conteúdo de uma comunicação é disponibilizado. Em outras palavras, é o elemento de rede no qual as informações trocadas entre dois ou mais usuários trafegam.
- *Administration Function* (ADMF): recebe o alvo a ser interceptado e ativa a interceptação no elemento de rede (IIF). Existe também uma ADMF no lado da autoridade que entrega o oficio judicial para operadora.
- *Mediation Function* (MF): realiza o serviço de conversão dos dados recebidos em um formato padronizado.

A comunicação entre esses elementos é realizada por dois tipos de interfaces. O primeiro grupo são as interfaces internas inerentes ao fabricantes dos equipamentos de rede (proprietárias), denominadas pela letra *X* ou pela sigla *Internal Network Interface* (INI). Já as interfaces pertencentes ao segundo grupo, são as interfaces denominadas de *Handover Interfaces* (HI) no qual os dados que trafegam por elas são encapsuladas no formato *Abstract Syntax Notation One* (ASN.1). Padrão que define como uma mensagem deve ser serializada.

A seguir é demonstrado uma pequena descrição de cada uma delas.

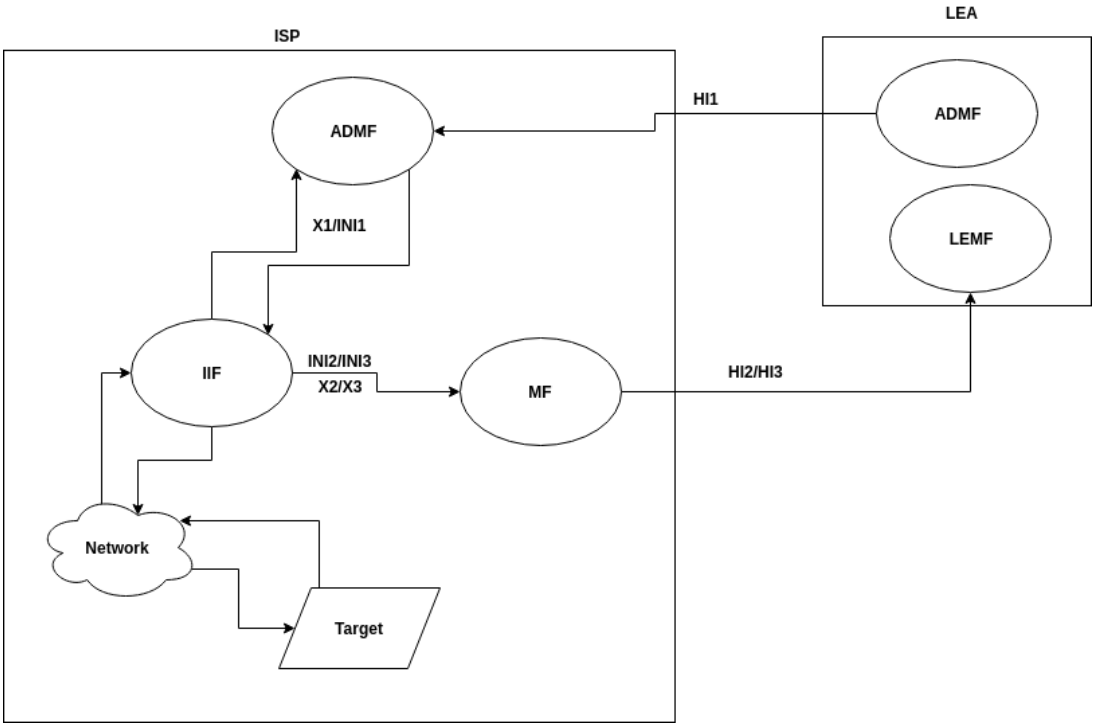
- X1 ou INI1: é por onde o alvo é configurado na IIF.
- X2 ou INI2: interface onde trafega o registro de conexão, o identificador e a localização do alvo, também chamado de *Intercept Related Information* (IRI).
- X3 ou IN3: é através dessa interface que as mensagens entre os usuários recebidas do IIF são transferidas ao MF.
- HI1: por onde trafega o dados coletados, referentes as informações da investigação. Sendo essas: o identificador do alvo, o identificador da interceptação (*Lawful Interception Identifier* (LIID)), o período de duração da interceptação e o endereço do LEMF que irá receber o HI2 e HI3.
- H12: por onde a IRI é entregue ao sistema da autoridade.
- HI3: interface de entrega do CC coletado.

2.3.1.2 Padrão ETSI TR 102 528

A norma define um modelo de interceptação em uma rede IP, semelhante a arquitetura demonstrada na 2.3.1.1. A diferença entre elas está na segmentação do IIF e da interface INI1. Acrescentou-se mais um elemento opcional: o CCTF. Abaixo será apresentado mais detalhes sobre esse novo modelo que pode ser observado na Figura 3.

- *Intercept Related Information Intercept Function* (IRI-IIF): elemento que se comunica com o gerador de IRI.
- *Content of Communication Intercept Function* (CC-IIF): elemento que providencia o conteúdo trocado entre os usuários.

Figura 2 – Arquitetura de um modelo de interceptação em uma rede genérica



Fonte: Adaptado de (ETSI, 2006b).

- CCTF: sua finalidade é determinar a localização do dispositivo CC-IIF e controlá-lo através da interface *Content of Communication Control Interface* (CCCI). O CCTF pode ser estaticamente provisionado pelo ADMF usando a interface INI1b ou dinamicamente controlado pelo IRI-IIF usando a interface *Content of Communication Trigger Interface* (CCTI). É possível, dependendo do cenário da rede, acrescentar o papel da CCTF a MF, e o IRI-IIF e o CC-IIF em um único elemento (ETSI, 2006a).

2.3.1.2.1 Cenários de interceptação

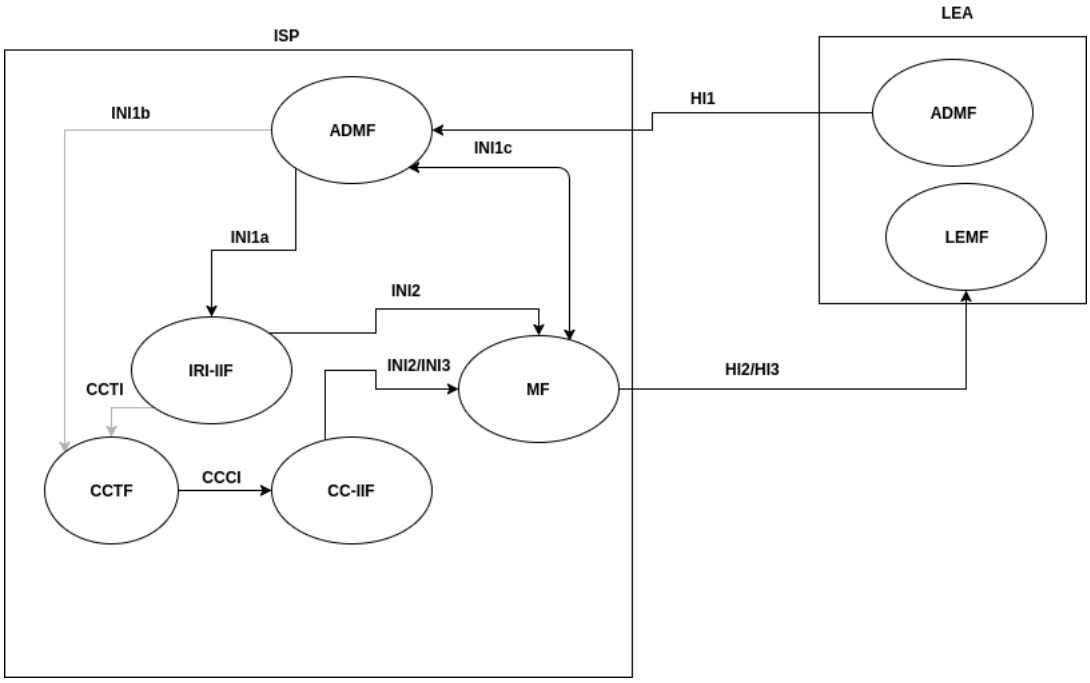
A norma prevê três possíveis cenários de interceptação demonstrados nas figuras a seguir. Na Figura 4 pode-se observar que há a presença do serviço de CCTF e o conteúdo é coletado do roteador que está diretamente ligado ao alvo. Já na Figura 5 o responsável por disponibilizar o CC é o *media gateway*. O último cenário demonstrado na Figura 6 o CCTF é realizado por um *hardware* à parte.

Os elementos apresentados nesses cenários realizam a comunicação entre a rede *comutada* por pacote (VoIP) e a *comutada* por circuito (*Rede Telefônica Comutada por Circuito* (RTCC)) também chamada de *Public Switched Telephone Network* (PSTN). Para melhor compreensão dos cenários os dois elementos que fazem esse papel serão descritos a seguir.

Um *media gateway* tem como finalidade repassar os fluxos de áudio entre a RTCC e a rede IP. Realiza a codificação e decodificação digital da voz em caso de transmissão analógica na rede RTCC (COLCHER, 2005). Em termos práticos é o responsável por converter os protocolos da rede IP para os protocolos da rede PSTN e vice-versa.

O *call agent* também denominado de *gateway de sinalização*, *softswitch* ou *Media Gateway Controller* (MGC) tem como papel traduzir as mensagens de sinalização da rede RTCC para a sinalização

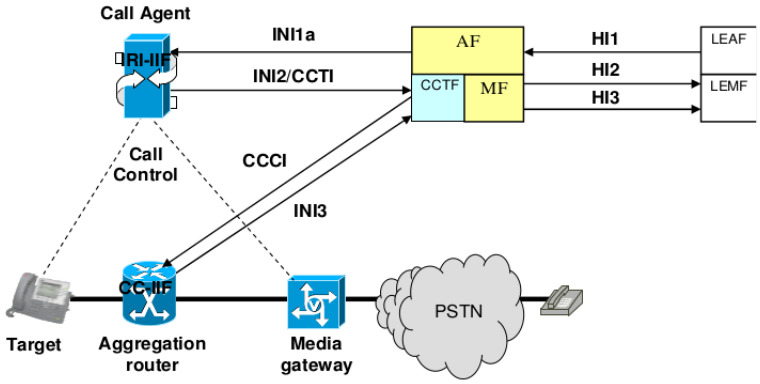
Figura 3 – Arquitetura de um modelo de LI em redes IP



Fonte: Adaptado de ETSI (2006a).

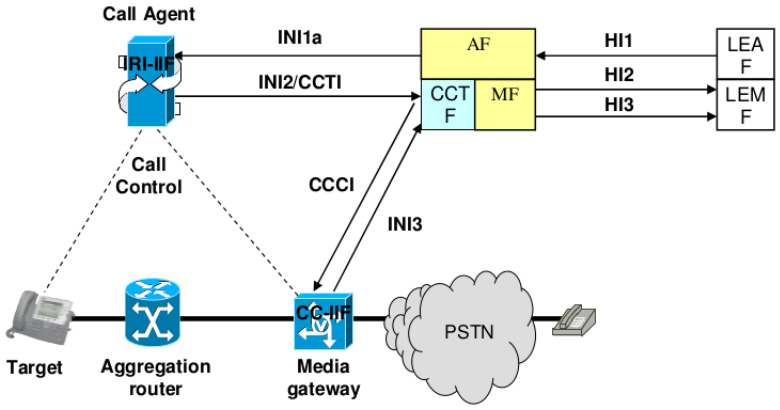
VoIP. Também é o responsável por controlar o *media gateway* para a geração da sinalização nos terminais da rede RTCC (COLCHER, 2005).

Figura 4 – Arquitetura VoIP onde o CC é coletado no roteador



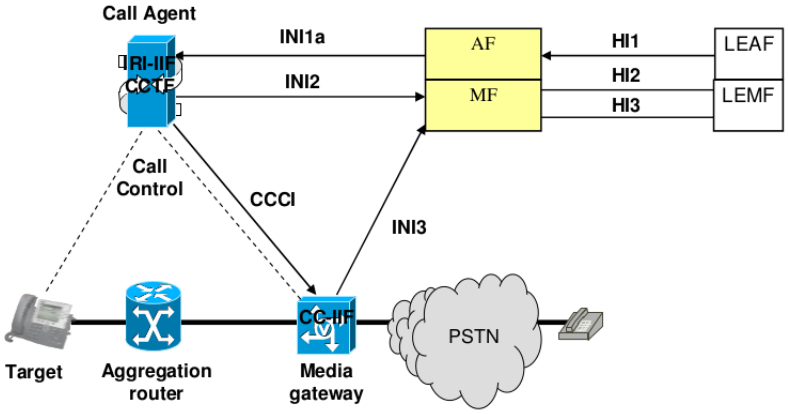
Fonte: ETSI (2006a).

Figura 5 – Arquitetura VoIP onde o CC é coletado no *media gateway*



Fonte: ETSI (2006a).

Figura 6 – Arquitetura VoIP onde o CCTF é um equipamento.

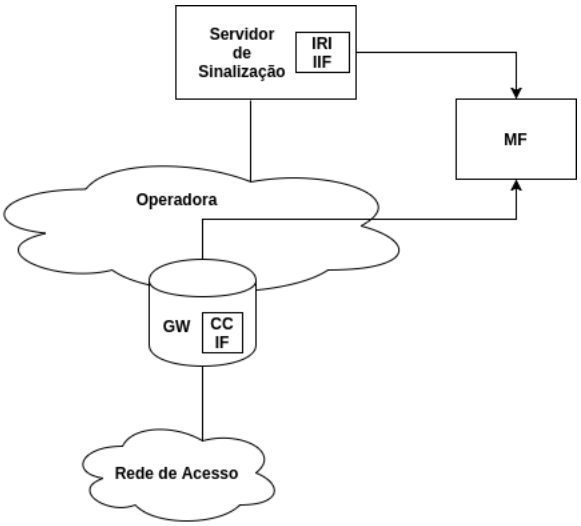


Fonte: ETSI (2006a).

2.3.2 Padrão ETSI TS 102 232-5

Essa norma demonstra quem é responsável por disponibilizar as informações de uma interceptação utilizando VoIP. Um dos protocolos presentes no VoIP responsável por determinar o identificador do usuário (IRI) através de seu URI é o SIP. Outro protocolo é o RTP de onde são extraídos os dados de uma comunicação (CC). Na Figura 7 é demonstrado um cenário utilizando esses protocolos, onde o SIP está presente no servidor de sinalização. E o RTP é capturado pelo *gateway/media gateway* da rede.

Figura 7 – Infraestrutura VoIP para serviços de LI



Fonte: Adaptado de (ETSI, 2019c).

2.3.3 *Communications Assistance for Law Enforcement Act* (CALEA)

O CALEA é uma lei americana aprovada em 1994, no qual regulamenta a interceptação das comunicações telemáticas. A partir da criação dessa lei surgiu o padrão ANSI J-STD-025-B que define tecnicamente o processo de interceptação (SÍCOLI, 2012).

2.3.3.1 Padrão ANSI J-STD-025-B

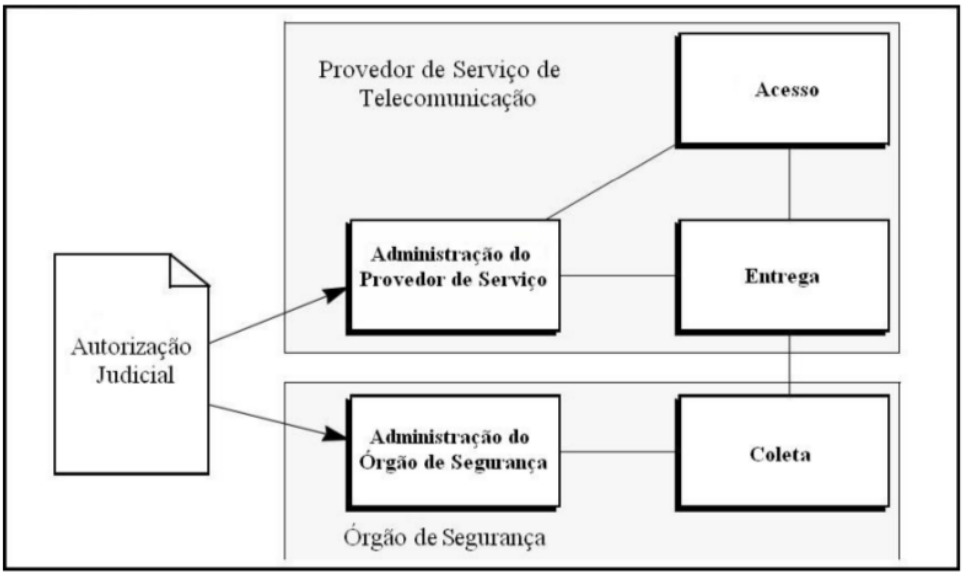
Esse padrão é similar aos padrões ETSI apresentados anteriormente, no qual tem-se os elementos que se localizam nas operadoras e na autoridade. Conforme apresentado na Figura 8 e segundo (SÍCOLI, 2012) os papéis desses elementos são:

- Administração do Provedor de Serviço: responsável por receber as informações do mandado judicial e controlar a função de acesso e entrega.
- Administração do Órgão de Segurança: encontra-se no escopo da autoridade e também armazena as informações do ofício judicial, fazendo a correlação entre essas informações e os dados interceptados através da função de coleta.
- Acesso: provê o acesso ao conteúdo da interceptação e aos dados de conexão, como a identificação dos usuários envolvidos na comunicação interceptada.
- Entrega: recebe os dados interceptados da função de acesso e as transmite para a função de coleta.
- Coleta: esse elemento faz o processamento e a análise dos dados interceptados.

2.4 Padrão brasileiro

O padrão brasileiro proposto pela ABNT para interceptação legal baseia-se nos padrões ETSI e será descrito no próximo tópico.

Figura 8 – Modelo definido pelo padrão ANSI J-STD-025-B



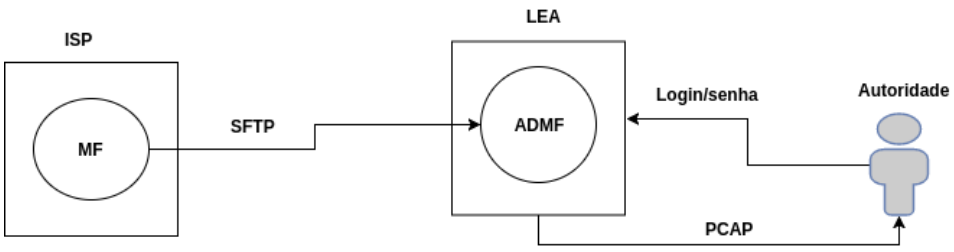
Fonte: (SÍCOLI, 2012).

2.4.1 Padrão ABNT-NBR 16386:2015

Descreve apenas como os dados interceptados serão entregues a autoridade. A interface de entrega do sistema de interceptação deverá utilizar o *SSH File Transfer Protocol* (SFTP), protocolo de transferência de arquivos. Os dados capturados deverão ser entregues no formato *PCAP* a entidade policial que solicitou a interceptação. O sistema responsável por armazenar essas informações deverá ter como método de autenticação *login* e senha (ABNT, 2015). O formato *PCAP* é um padrão utilizado na maioria dos sistemas de captura de pacotes de rede, como o *Wireshark* e *Tcpdump*.

Fazendo uma analogia as normas ETSI tem-se o MF na operadora que entrega os dados em formato *PCAP* para o sistema da autoridade (ADMF), via protocolo SFTP. O acesso ao ADMF será apenas por *login* e senha. A Figura 9 apresenta essa comparação.

Figura 9 – Comparação entre o padrão brasileiro e o padrão europeu



Fonte: Próprio autor.

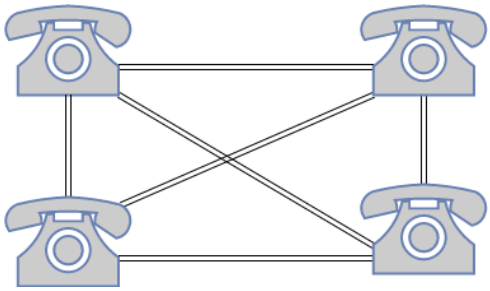
2.5 O sistema telefônico

Alexander Graham Bell e seu ajudante Thomas A. Watson foram os responsáveis por inventarem o primeiro sistema telefônico, no qual os usuários eram ligados diretamente por linhas dedicadas, como mostrado na Figura 10. Com o crescimento das linhas telefônicas foi necessário criar um elemento que centralizasse essas linhas (circuitos), surgindo então o elemento mais importante de uma rede de telefonia,

a central telefônica (COLCHER, 2005).

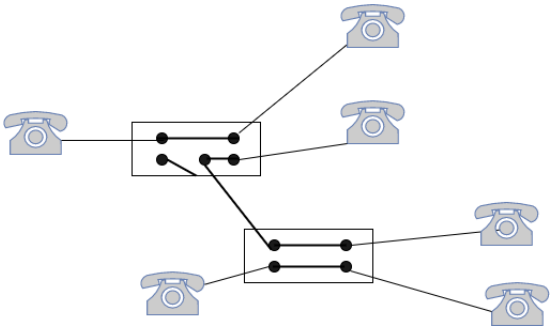
O papel da central telefônica é realizar a *comutação* dos *circuitos* a fim de estabelecer a comunicação entre dois ou mais assinantes, como mostrado na Figura 11 (COLCHER, 2005).

Figura 10 – Primeiro sistema telefônico



Fonte: Próprio autor.

Figura 11 – Central telefônica



Fonte: Adaptado de (COLCHER, 2005).

2.5.1 Evolução do sistema telefônico

Nas primeiras centrais o *chaveamento* era realizado de forma manual, no qual operadores humanos (telefonistas) recebiam pedidos de ligações e fechavam fisicamente os circuitos entre o chamador e o chamado, por meio de cabos e conexões (COLCHER, 2005). Como demonstrado na Figura 12.

Figura 12 – Telefonista responsável por realizar a *comutação* de forma manual

Fonte: (GALILEU, 2013).

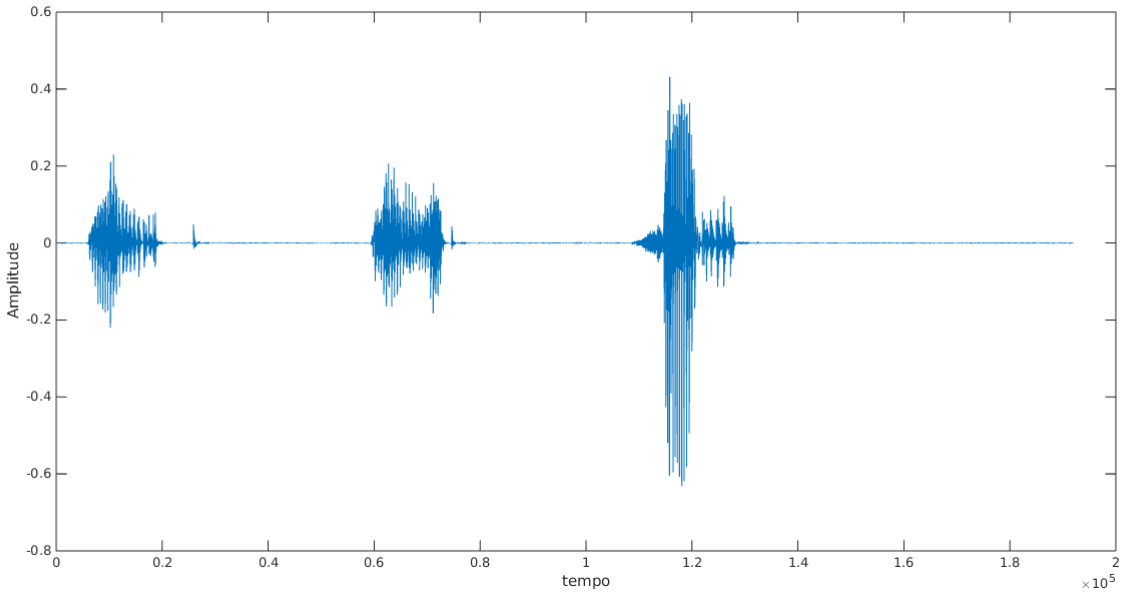
Em 1891 a primeira central automática foi invetada por Almon Strowger. A *comutação* desse dispositivo era realizada através de elementos eletromecânicos e não mais por humanos (COLCHER, 2005). Após a criação do primeiro transistor e com a evolução dos sistemas eletrônicos foi possível realizar a digitalização das centrais telefônicas.

2.5.1.1 Telefonia digital

Surgimento da *Central de Programa Armazenado* (CPA) responsável por realizar a *comutação* entre usuários através de um sistema computacional. O sinal analógico (voz) é convertido em um sinal digital para ser processado e transmitido por essas centrais.

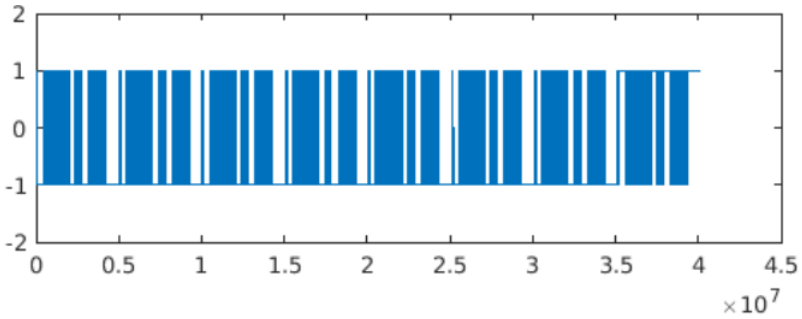
Um sinal analógico é um sinal que pode assumir inúmeros valores ao longo do tempo, podendo variar continuamente. A Figura 13 é um exemplo desse tipo de sinal. Já o sinal que assume um conjunto de possíveis valores é denominado de sinal digital e está representado pela Figura 14.

Figura 13 – Exemplo de um sinal analógico elaborado na ferramenta *Matlab*



Fonte: Próprio autor.

Figura 14 – Exemplo de um sinal digital elaborado na ferramenta *Matlab*



Fonte: Próprio autor.

2.5.1.1.1 Conversão analógica digital

A conversão de um sinal analógico para digital, processo conhecido como *Pulse Code Modulation* (PCM), toma como base o teorema de Nyquist. Ele determina que um sinal com banda B Hz, para ser recuperado, precisa de uma taxa de amostragem igual ou maior que $2B$. Após determinada essa taxa, a amplitude do sinal analógico é fragmentado em uma quantidade de N amostras. Cada amostra é aproximada a um número inteiro de n bits, mecanismo denominado de quantização. Existem dois tipos principais: a quantização linear, em que os níveis de quantização são igualmente espaçados e a quantização logarítmica. Nesse último o sinal sofre uma transformação logarítmica de acordo com as fórmulas a seguir: lei A (Equação 2.1 e Equação 2.2) e lei μ (Equação 2.3) (COLCHER, 2005).

$$y(x) = \begin{cases} \frac{1+ln(Ax)}{1+ln(A)} & para \quad \frac{1}{A} < x < 1 \end{cases} \tag{2.1}$$

$$y(x) = \begin{cases} \frac{Ax}{1+ln(A)} & para \quad 0 < x < \frac{1}{A} \end{cases} \tag{2.2}$$

$$y(x) = \begin{cases} \frac{ln(1+\mu x)}{ln(1+\mu)} \end{cases} \qquad 0 < x < 1 \tag{2.3}$$

Alguns *codecs* de áudio utilizam essas equações em seu algoritmo de compressão. Como é o caso do G.711, apresentado na seção 5

2.5.1.2 Sinalização

A sinalização é o processo de troca de informações entre os elementos de um sistema de telecomunicações, como propósito: estabelecer uma conexão e gerenciar os recursos e estado desse sistema (COLCHER, 2005). Ela pode ser classificada da seguinte forma:

2.5.1.2.1 Sinalização de supervisão

Nessa sinalização são enviadas informações sobre o estado das linhas, conexões e equipamentos. Por exemplo, se um circuito ou terminal do usuário está livre ou ocupado. Esses sinais também podem ser enviados entre centrais (*sinalização de linha*) (COLCHER, 2005).

2.5.1.2.2 Sinalização de indicação ao usuário

Sinalização destinada ao usuário final, cuja finalidade é informar o estado do sistema telefônico (COLCHER, 2005). Os principais tipos são:

- Tom de discar: sinal recebido pelo usuário que deseja iniciar uma chamada, indicando que ele inicie uma ligação através da discagem do número do receptor.
- Tom de controle da chamada: sinal emitido para informar que o terminal do receptor está livre e sendo chamado.
- Tom de ocupado: indica que o estabelecimento da comunicação não foi completado ou o usuário chamado não atendeu a ligação.
- Rede inacessível: sequência de tons, podendo ser uma mensagem gravada pelo operadora de telefonia, que indica ao usuário que fez a chamada que não é possível estabelecer a comunicação.
- Corrente de toque: sinal enviado pelo central telefônica ao terminal receptor indicando que uma ligação com esse terminal foi estabelecida, em outras palavras, é o toque sonoro que um aparelho telefone recebe quando um usuário deseja conversar com o proprietário do aparelho.

2.5.1.2.3 Sinalização de numeração

Encaminha os pedidos de estabelecimento de conexões a partir do assinante que estabeleceu uma ligação até o destinatário. Na linha do assinante a sinalização de numeração mais conhecida é o *Dual-tone Multifrequency* (DTMF). Este tipo de sinalização está presente no aparelho telefônico, onde cada tecla do aparelho corresponde a uma frequência diferente (COLCHER, 2005).

2.6 *Voice Over Internet Protocol* (VoIP)

È um conjunto de tecnologias relacionados à comunicação de voz sobre o protocolo IP (COLCHER, 2005). Os protocolos VoIP mais conhecidos são: protocolo SIP e RTP.

2.6.1 *Session Initiation Protocol* (SIP)

O SIP é o protocolo de sinalização de nível de aplicação, responsável por iniciar e gerenciar uma sessão de comunicação entre um ou mais usuários para troca de mídias (COLCHER, 2005).

Segundo (COLCHER, 2005) uma arquitetura de sinalização SIP é composta pelos seguintes elementos:

- UA (*Agente usuário*): formado pelo terminal do *User Agent Client* (UAC) e pelo *User Agent Server* (UAS). O UAC faz a requisição de mensagens SIP. O UAS processa e responde a essas requisições.
- *Servidor proxy (proxy server)*: elemento intermediário responsável por gerar requisições SIP para clientes que não podem fazer essas requisições diretamente. Ao receber uma requisição ele identifica o usuário de destino e encaminha a mensagem para esse assinante.
- *Servidor de redirecionamento (redirect server)*: auxilia o servidor *proxy* na localização do usuário, responde ao UA de origem qual o endereço mais próximo do UA de destino.
- *Servidor de registro (registrar server)*: armazena a localização de algum elemento da rede, trabalha em conjunto com os servidores *proxy* e de redirecionamento.

2.6.1.1 Identificação do usuário

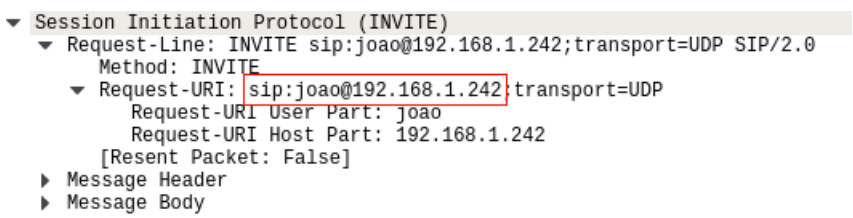
A identificação de um usuário no protocolo SIP segue o esquema de endereçamento baseado no identificador URI. Utiliza o *Uniform Resource Locator* (URL) semelhante a utilizada em serviços de correio eletrônico (COLCHER, 2005). Uma URI é um identificador de um recurso (áudio, imagem, vídeo, texto, usuário) em uma rede. Já uma URL são as informações de localização de um recurso, como IP e porta (IETF, 2005). Uma URL é o subconjunto de uma URL como demonstrado na Figura 15.

A estrutura básica de um URI SIP é mostrada na Figura 16, onde está presente a identificação do protocolo, o identificador do usuário e seu IP.

Figura 15 – Estrutura geral de uma URI

Fonte: Próprio autor.

Figura 16 – Estrutura de uma URI SIP



Fonte: Próprio autor.

2.6.1.2 Mensagens SIP

A seguir será apresentado as principais mensagens enviadas para o estabelecimento de uma sessão SIP. A Tabela 2 apresenta o conjunto dos principais métodos SIP e a Tabela 3 são as principais classes de respostas que um servidor SIP pode enviar de acordo com a requisição recebida.

Tabela 2 – Principais métodos para estabelecimento de uma sessão SIP

Método	Funcionalidade
`INVITE`	Representa uma requisição de convite para determinado usuário participar de uma sessão.
`ACK`	Mensagem de confirmação da requisição `INVITE`.
`BYE`	Solicita o término da sessão estabelecida.
`CANCEL`	Solicita o cancelamento de uma sessão antes do término da comunicação.
`REGISTER`	Registra as informações de um usuário no servidor de registro.

Fonte: Adaptado de (COLCHER, 2005).

Tabela 3 – Principais respostas dos servidores SIP

Classe	Funcionalidade	Exemplo
`1xx`	Resposta informativa.	`180 Ringing`
`2xx`	Resposta de sucesso na requisição.	`200 OK`
`3xx`	Resposta de redirecionamento.	`302 Moved Temporarily`
`4xx`	Falha na requisição.	`404 Not Found`
`5xx`	Falha no servidor.	`503 Service Unavailable`

Fonte: (COLCHER, 2005).

2.6.2 *Session Description Protocol* (SDP)

Responsável pelo processo de negociação da mídia e outras informações relacionadas a ela (COLCHER, 2005). O SDP é carregado junto ao protocolo de sinalização.

A descrição dessas informações é representada na forma textual através da codificação *Unicode Transformation Format* (UTF-8), apenas o nome dos campos e atributos são codificados em *American Standard Code for Information Interchange* (US-ASCII). A estrutura dessas informações é realizada da seguinte forma: `tipo-do-campo=valor-do-campo` (COLCHER, 2005). A Tabela 4 apresenta os atributos obrigatórios na descrição de uma sessão.

Tabela 4 – Campos do protocolo SDP

Campo	Descrição
`v`	Versão do protocolo.
`o`	Identificador do criador da sessão.
`s`	Nome da sessão.
`t`	Tempo que a sessão está ativa, informando o horário de início e término.
`m`	Informa o nome da mídia, o endereço, a porta e protocolo de transporte para qual a mídia deve ser enviada.

Fonte: Adaptado de (COLCHER, 2005).

2.6.2.1 *Codecs*

Para ser possível realizar a transmissão de um áudio utilizando a tecnologia VoIP é necessário o uso de *codecs* que realizam a conversão do sinal de voz em um sinal digital. A Tabela 5 apresenta alguns dos principais *codecs* e suas respectivas taxas de amostragem.

Tabela 5 – *Codecs* de áudio

Codec	**Taxa de amostragem**
G.711 (Lei μ)	8 kHz
G.711 (Lei A)	8 kHz
G723	8 kHz
L16	44,1 kHz

Fonte: Adaptado de (COLCHER, 2005).

2.6.3 *Real-time Transport Protocol* (RTP)

Protocolo responsável pela transmissão da mídia (áudio, vídeo, texto) por aplicações que utilizam fluxos de dados em tempo real. Usa em maioria dos casos o protocolo de transporte UDP e o protocolo RTCP como protocolo de controle. Estabelecendo portanto um canal de transmissão para troca de mídia entre usuários. O pacote RTP não oferece nenhum mecanismo de garantia de entrega e qualidade de serviço. Os pacotes podem chegar desordenados, o receptor reconstrói a informação pelo número de sequência contido em cada pacote (IETF, 2003).

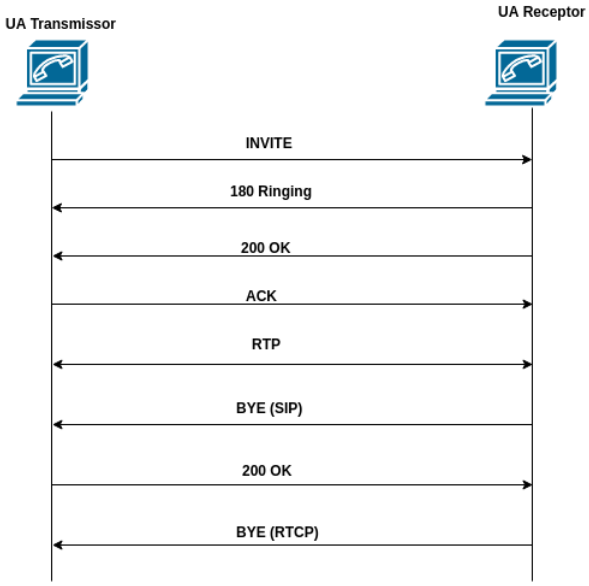
2.6.3.1 *Real-time Control Protocol* (RTCP)

È responsável por prover informações de qualidade de uma sessão RTP, por meio da transmissão periódica de pacotes de controle para todos os participantes da sessão (COLCHER, 2005). Segundo (ARNDT, 2009) algumas das mensagens enviadas nesses pacotes, são:

- *Sender Report* (SR): mensagem gerada pelo transmissor da mídia contendo a quantidade dos pacotes que foram transmitidos.
- *Receiver Report* (RR): informações relativas a taxa de perda de pacotes e *jitter* enviadas pelo participante ativo de uma sessão RTP.
- *BYE*: indica o fim de uma sessão.

A Figura 17 apresenta o fluxo de comunicação entre dois agentes (usuários) desde o estabelecimento da sessão SIP até a transmissão da mídia.

Figura 17 – Estabelecimento de uma ligação VoIP entre dois UAs



Fonte: Próprio autor.

A implementação de uma interceptação legal não é algo trivial a ser realizado, pois envolve um conjunto de fatores que partem desde o contexto legal a infraestrutura das operadoras de telecomunicações. Como descrito neste trabalho uma rede de telefonia é composta por diversos tipos de elementos que realizam determinados papéis. Um sistema telefônico pode ser composto apenas por uma central e terminais de usuários ou por dispositivos que permitem a interligação entre a rede PSTN e a rede IP. Por esse motivo este trabalho visa apenas atender a telefonia IP, não abordando outras infraestruturas de telefonia.

3 PROPOSTA DE TRABALHO

Ao longo deste capítulo serão apresentadas tecnologias de baixo custo para a realização de interceptações em centrais telefônicas IP, em especial nos pequenos provedores que oferecem serviços de telefonia IP. Para alcançar os objetivos propostos neste trabalho a metodologia foi dividida em quatro etapas: estudo de padrões e tecnologias de automatização, estudo dos equipamentos VoIP, implementação de um cenário de interceptação e por fim a execução de uma interceptação e desvio de uma ligação VoIP.

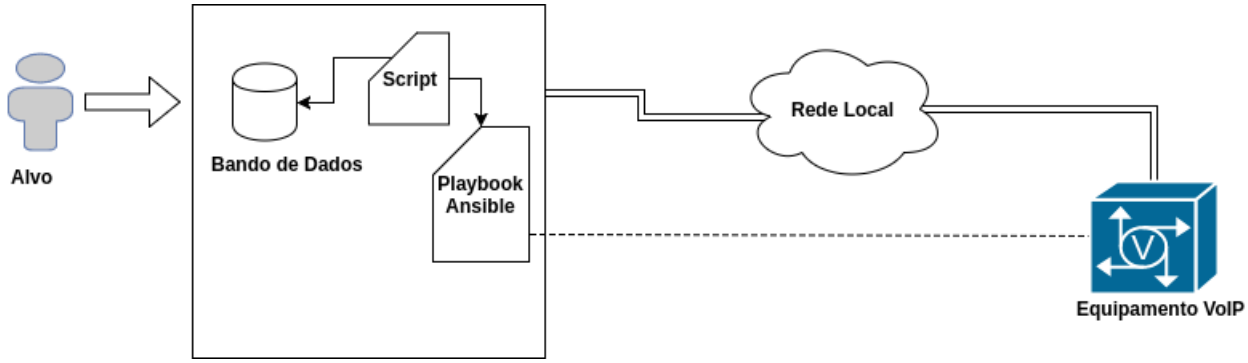
3.1 Metodologia

3.1.1 Estudo de padrões e tecnologias de automatização

Nessa etapa serão estudadas as ferramentas utilizadas para automatização de equipamentos de rede. A função da ferramenta escolhida será configurar o(s) equipamento(s) utilizado(s) na implantação do cenário escolhido, passando como parâmetro o identificador(es) do alvo(s) a ser(em) interceptado(s). Também será determinado a linguagem de programação que será empregada como mecanismo auxiliar no processo de interceptação. As possíveis ferramentas serão: *Ansible* para o processo de automatização e linguagens de programação como *Python* e C++. Não será abordado neste estudo meios de automatização de cadastro e armazenamento de ofícios judiciais. O único dado do ofício que será cadastrado e de forma manual será o identificador do alvo sob investigação.

Será desenvolvido um *script* na linguagem de programação escolhida que ficará esperando o cadastro de novos alvos. Ele será responsável pela criação e execução do *playbook*, que é a descrição das etapas de configuração a serem executadas pela ferramenta *Ansible*. Nessa etapa também será definido o banco de dados, assim como a modelagem do mesmo, cujo fim será o armazenamento dos alvos cadastrados e das informações extraídas da interceptação. A Figura 18 demonstra esse procedimento.

Figura 18 – Tecnologias utilizadas para automatização de uma LI



Fonte: Próprio autor.

3.1.2 Estudo dos equipamentos VoIP

Será realizada a leitura dos manuais de alguns equipamentos comerciais, com o objetivo de analisar como esses elementos realizam o processo de interceptação e qual são os protocolos utilizados para esse fim. Nessa fase também serão estudadas tecnologias, preferencialmente *open source*, para a implantação de um servidor SIP e um *Internet Protocol Private Branch Exchange* (IP PBX).

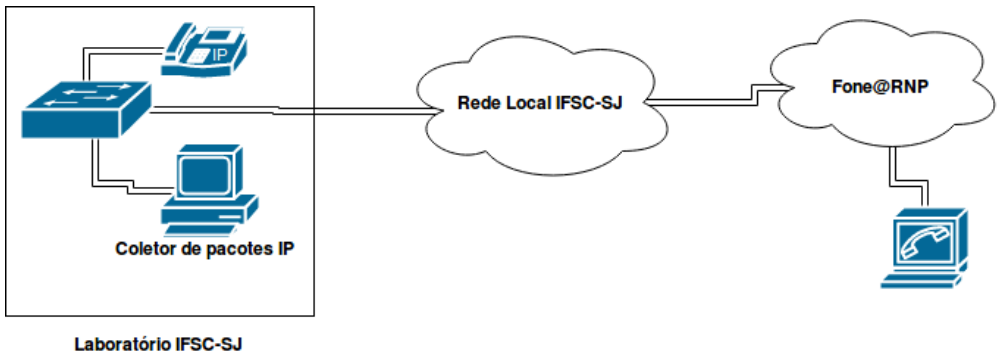
3.1.3 Implementação de um cenário de interceptação

O objetivo dessa fase é implantar um cenário com as tecnologias VoIP estudadas na seção 3.1.2. Em um primeiro momento foi cogitado utilizar um *switch* CISCO *catalyst* 2940, que seria instalado no laboratório de iniciação científica do IFSC-SJ e conectado a rede de telefonia da Rede Nacional de Ensino e Pesquisa (*Fone@RNP*). No *switch* seria conectado um telefone IP, ou *softphone* e na rede da RNP seria ligado outro aparelho. Uma ligação entre os dois telefones seria realizada e com um computador conectado no *switch* seria feita a captura dos pacotes IP. A Figura 19 apresenta como seria a implantação desse primeiro cenário.

Mas fazendo uma análise chegou-se a conclusão que realizar a captura dos pacotes diretamente no *switch* seria muito mais complexo construir uma aplicação que realizasse a extração dos pacotes SIP e RTP. Pacotes cifrados também seriam um problema, pois sem acesso as chaves de segurança não seria possível retirar qualquer informação - considerando tempo hábil de processamento. Por questões burocráticas também seria difícil utilizar a rede da *Rede Nacional de Ensino e Pesquisa* (RNP), por esses motivos optou-se em implantar um cenário próprio.

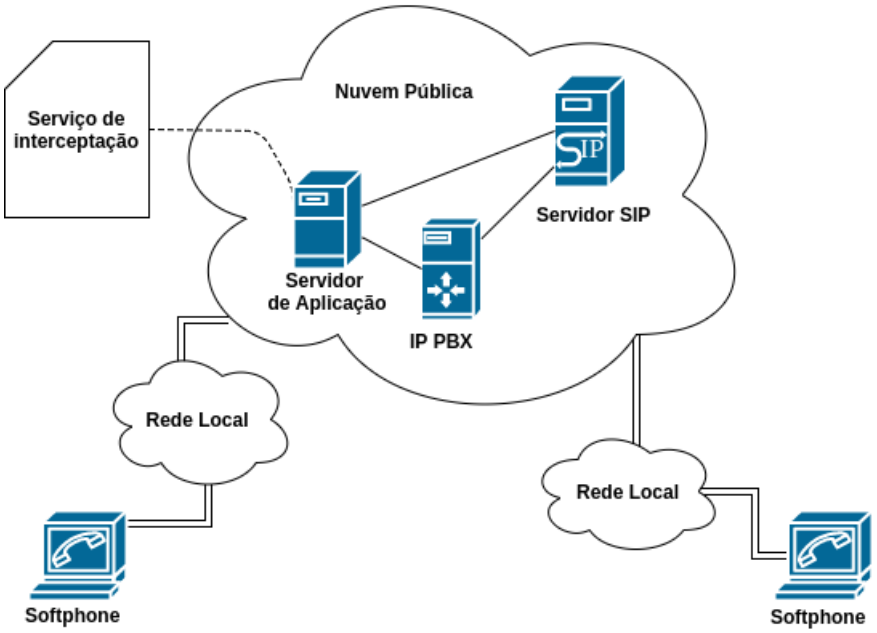
Para a implantação dessa rede serão estudadas formas de implantar os serviços VoIP em nuvens públicas, como *AWS* e *Google cloud*. Também será realizado um estudo de implantação na própria rede do IFSC-SJ, que oferece acesso externo. O objetivo de colocar esses serviços em *nuvem* é de ter baixo custo, pois servidores com um bom poder de processamento possuem um valor elevado. Outra vantagem é por causa da terceirização da infraestrutura. Sob o ponto de vista de segurança, isso será um ponto que será analisado no andamento dessa tarefa. Basicamente será implantado nessas plataformas um servidor SIP e um IP PBX, ambos configurados com um IP público. E por fim será implantado um servidor que estará executando os serviços de interceptação. Dois *softphones* conectados a uma outra rede terão acesso a esses equipamentos e poderão realizar uma ligação entre si (ver Figura 20).

Figura 19 – Cenário utilizando a rede da RNP



Fonte: Desenvolvida pelo próprio autor.

Figura 20 – Infraestrutura da rede VoIP utilizando plataformas de serviços em *nuvem*



Fonte: Desenvolvida pelo próprio autor.

3.1.4 Execução de uma interceptação e desvio de uma ligação VoIP

Será desenvolvido um serviço de interceptação com base nos modelos apresentados nas normas estudadas. Esse serviço terá como função a execução da configuração dos equipamentos VoIP e irá extrair as informações de IRI e CC dos pacotes coletados.

3.1.5 Cronograma

A Tabela 6 apresenta o cronograma das tarefas, nomeadas com a letra T seguidas de sua numeração correspondente, que são previstas para o cumprimento dos objetivos relatados neste trabalho. A seguir são apresentadas essas atividades.

- T1: Estudo das ferramentas de automatização.
- T2: Estudos dos manuais dos equipamentos e tecnologias VoIP.
- T3: Implantação da infraestrutura dos serviços.
- T4: Implementação de testes com as ferramentas de automatização.
- T5: Desenvolvimento do serviço de interceptação.
- T6: Escrita final da monografia.

Tabela 6 – Cronograma de tarefas

Tarefas	**Mês**					
	Julho	**Agosto**	**Setembro**	**Outubro**	**Novembro**	**Dezembro**
T1						
T2						
T3						
T4						
T5						
T6						

3.2 Considerações finais

Automatizar um processo de interceptação legal será um grande desafio, pois será implementado uma infraestrutura VoIP em *nuvem* que utiliza a pilha de protocolos TCP/IP, consequentemente herdando os problemas conhecidos dessa rede, como latência e perda de pacotes. Pacotes RTP e SIP estarão suscetíveis a essas perdas, o que dificultará a extração das informações necessárias para a implementação da interceptação. Isto afetará o desempenho do sistema. Outro fator que deverá ser analisado é a questão da privacidade e segurança das plataformas de nuvem, pois como foi citado ao longo deste trabalho a legislação brasileira é bem clara enquanto ao vazamento das informações coletadas.

REFERÊNCIAS

ABNT. *NBR 16386:2015*. [S.l.: s.n.], 2015. Citado na página 23.

ANATEL. *Telefonia Móvel - Acessos*. 2019. Disponível em: <http://www.anatel.gov.br/dados/acessos-telefonia-movel>. Citado na página 13.

ARNDT, D. *Estudo e implantação do sistema de telefonia VoIP no CEFET-SC integrado ao serviço fone@RNP*. [S.l.: s.n.], 2009. Citado na página 30.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Citado na página 15.

BRASIL. *Lei Nº 9.296, de 24 de julho de 1996*. 1996. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Citado na página 15.

BRASIL. *LEI Nº 12.965, DE 23 DE ABRIL DE 2014*. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Citado na página 16.

CNJ. *Resolução nº 59, de 09 de setembro de 2008*. 2008. Disponível em: <http://www.cnj.jus.br/busca-atos-adm?documento=2602>. Citado na página 16.

COLCHER, S. e. a. *VoIP Voz sobre IP*. [S.l.: s.n.], 2005. Citado 9 vezes nas páginas 19, 20, 24, 25, 26, 27, 28, 29 e 30.

ETSI. *Lawful Interception (LI)*. 1995. Disponível em: <https://www.etsi.org/technologies/lawful-interception>. Citado na página 15.

ETSI. *ETSI TR 102 528*. [S.l.: s.n.], 2006. Citado 4 vezes nas páginas 17, 19, 20 e 21.

ETSI. *Lawful Interception (LI); Concepts of Interception in a Generic Network Architecture*. [S.l.: s.n.], 2006. Citado 3 vezes nas páginas 13, 17 e 19.

ETSI. *About ETSI - A European Standards Organization with Global Impact*. 2019. Disponível em: <https://www.etsi.org/about>. Citado na página 13.

ETSI. *ETSI members around the world*. 2019. Disponível em: <https://www.etsi.org/membership/members>. Citado na página 17.

ETSI. *Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services*. [S.l.: s.n.], 2019. Citado 2 vezes nas páginas 17 e 22.

GALILEU, R. *Bem antes do iPhone*. 2013. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI269863-17773,00-BEM+ANTES+DO+IPHONE.html>. Citado na página 25.

GUARDIA, G. *Comunicações Eletrônicas e Dados Digitais no Processo Penal*. [S.l.: s.n.], 2012. Citado na página 15.

IETF. *RFC 3550 - RTP: A Transport Protocol for Real-Time Applications*. [S.l.: s.n.], 2003. Citado na página 30.

IETF. *RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax*. [S.l.: s.n.], 2005. Citado na página 28.

SÍCOLI, F. *Uma Proposta de Modelo para Transmissão de Dados Interceptados na Internet Brasileira*. [S.l.: s.n.], 2012. Citado 2 vezes nas páginas 22 e 23.