Plataforma Smartspace

Funcionalidades Comuns

Documentação Técnica
v. 2.23.4

Conteúdo

1 Apresentação da Solução 3

2 Módulos da Plataforma 4

2.1 Smartspace Voice 4

2.1.1 SIP Server 4

2.1.2 BD Server 5

2.1.3 VoiceMail Server 5

2.1.4 Fax Server 5

2.2 Smartspace Collab 5

2.2.1 Smartspace Communication Server 6

2.2.2 Smartspace IM Server 6

2.2.3 Smartspace Squad 6

2.3 Smartspace Contact Center 6

2.3.1 Smartspace Metrics 7

2.3.2 Smartspace IVR Server 7

2.3.3 Smartspace Record 7

2.4 SMARTSPACE Manager/Monit 8

2.5 TARIF – Sistema de Tarifação e Gestão de Telecom 8

3 Características Gerais 10

4 Arquitetura 18

4.1 Alta Disponibilidade e Redundância 18

4.1.1 Especificações técnicas 19

4.1.2 Sobrevivência local 36

5 Criptografia e Segurança 37

5.1 Especificações Técnicas 38

6 Licenciamento 41

7 RFCs e padrões de Mercado 45

8 Informações de hardware 49

8.1 Especificações técnicas 49

1 Apresentação da Solução

A Plataforma **SMARTSPACE** é uma solução de Comunicação Unificadas e Engajamento Omnichannel, reconhecida como referência no mercado. Utilizando protocolos padrão de mercado como SIP, WebRTC e XMPP, a plataforma combina tecnologia de ponta, flexibilidade e segurança para atender aos mais exigentes cenários de comunicação corporativa. Desenvolvida pela Smartspace, a solução oferece uma interface 100% WEB, em Português do Brasil, que proporciona simplicidade, eficiência e agilidade na administração de ambientes de comunicação unificada.

Nos últimos três anos, a Plataforma SMARTSPACE foi destacada por sua excelência ao receber consecutivamente o prêmio '**Best Communications Platform Solution**' do Brasil da **Frost & Sullivan** (2022, 2023 e 2024). Esses reconhecimentos consolidam a liderança da Smartspace como uma fornecedora de soluções inovadoras e de alto impacto no mercado de comunicações unificadas.

Projetada com os mais altos padrões de segurança e confiabilidade, a Plataforma SMARTSPACE é certificada pelas normas **ISO 27001** e **ISO 27701**, garantindo que todos os seus sistemas, processos e produtos estejam em conformidade com as melhores práticas de privacidade e proteção de dados. Essas certificações refletem o compromisso inabalável da Smartspace em oferecer uma solução robusta e confiável.

A plataforma foi desenvolvida para atender projetos de qualquer porte, desde operações em uma única localidade até projetos multi-sites com redundância geográfica e requisitos avançados. Essa versatilidade, aliada a uma arquitetura multi-tenant, permite à Smartspace se adaptar perfeitamente a diferentes necessidades de negócios.

Através da Plataforma SMARTSPACE, é possível gerenciar, manter e monitorar todas as operações de comunicação unificada de maneira centralizada, seja pela CLI (linha de comando) ou por uma interface web unificada e intuitiva.

A Plataforma SMARTSPACE é composta por módulos integrados e independentes, projetados para trabalhar em conjunto ou separadamente, dependendo das necessidades do cliente. Além disso, a Smartspace disponibiliza uma linha completa de equipamentos com marca própria – incluindo gateways e SBC fabricados em parceria com a Audiocodes e telefones IP desenvolvidos em parceria com Yealink e Intelbras – todos homologados pela ANATEL, oferecendo soluções completas e integradas.

Todos os módulos da Plataforma SMARTSPACE são multi-idiomas, com suporte para Português do Brasil, Inglês e Espanhol, o que facilita sua implementação em diferentes mercados e contextos.

Com licenciamento centralizado e flexível, a solução garante total mobilidade para os usuários, permitindo que eles acessem seus recursos de qualquer localidade, sem perda de funcionalidades.

A Smartspace investe continuamente na evolução e melhoria da plataforma, assegurando que seus clientes tenham acesso às mais recentes inovações e melhorias por meio do sistema de HelpDesk (https://digivox.smartspace.cx). O processo de atualização é simplificado, podendo ser realizado de forma automática ou manual, sem necessidade de reinstalar o sistema. Além disso, o HelpDesk oferece um suporte completo, permitindo abertura de chamados, acesso à base de conhecimento, consulta à documentação técnica e outras funcionalidades que promovem uma experiência superior.

2 Módulos da Plataforma

A Plataforma SMARTSPACE é uma suíte de aplicativos completa e 100% baseada em software, projetada para atender desde sistemas de comunicação em tempo real até avançados recursos de gestão de telecom. Essa arquitetura flexível e moderna reflete o compromisso da Smartspace em oferecer soluções de ponta que se adaptam perfeitamente às diversas demandas do mercado.

A modularidade é um dos principais diferenciais da Plataforma SMARTSPACE. Seus módulos podem operar de forma totalmente integrada, criando um ecossistema coeso, ou funcionar de maneira independente, dependendo das necessidades específicas da arquitetura adotada. Essa flexibilidade permite à plataforma atender desde pequenas implementações até grandes projetos corporativos, garantindo máxima eficiência e escalabilidade.

O processamento dos recursos da plataforma é distribuído em diversos componentes que podem ser instalados em um único servidor para projetos compactos ou alocados em servidores dedicados para cada serviço em projetos de maior porte. Essa abordagem modular e escalável garante alta performance e confiabilidade para qualquer topologia escolhida.

A seguir, detalhamos cada componente e suas características exclusivas.

2.1 Smartspace Voice

O Smartspace Voice é o módulo de comunicação central da Plataforma SMARTSPACE, atuando como um poderoso Softswitch SIP. Baseado nativamente no padrão SIP RFC3261, ele é responsável pelo registro, controle e gerenciamento de sessões SIP e WebRTC de todos os elementos da solução, oferecendo alta eficiência, escalabilidade e confiabilidade. Este módulo é projetado para atender às necessidades mais exigentes de comunicação empresarial, suportando ambientes de pequeno a grande porte, com total aderência às melhores práticas do mercado.

O Smartspace Voice é composto pelos seguintes módulos:

2.1.1 SIP Server

O Smartspace SIP Server é o núcleo do módulo Voice e desempenha um papel crítico na operação da plataforma. Ele é:

- Totalmente baseado em software, garantindo flexibilidade e facilidade de implantação.
- Gerenciado através de uma interface WEB intuitiva, que simplifica sua administração.
- Compatível com todos os padrões definidos na RFC SIP 3261, assegurando interoperabilidade com outros sistemas SIP.

Suas responsabilidades incluem:

- Controle completo das chamadas, incluindo estabelecimento, roteamento e finalização.
- Gerenciamento de controle de admissão de chamadas (CAC), para otimização do uso dos recursos.

- Integração com gateways remotos (SIP), ampliando a conectividade da solução.
- Registro de endpoints e/ou gateways, garantindo alta disponibilidade para os usuários.
- Autorização de chamadas e controle de funcionalidades SIP avançadas.

2.1.2 BD Server

O BD Server é o servidor de banco de dados único da plataforma, essencial para o armazenamento seguro e eficiente de informações. Ele é construído sobre o robusto PostgreSQL, oferecendo suporte a:

- Replicação multi-master, que assegura alta disponibilidade e confiabilidade dos dados.
- Armazenamento de dados de configuração, registros de chamadas (CDRs), regras de roteamento e informações de usuários.
- Escalabilidade para atender demandas crescentes, sem comprometer o desempenho.

2.1.3 VoiceMail Server

O VoiceMail Server é responsável pela gestão das caixas postais da plataforma, oferecendo:

- Processamento completo das mensagens de voz dos usuários.
- Integração perfeita com os demais módulos do Smartspace Voice, proporcionando uma experiência de comunicação fluida.
- Recursos que permitem o acesso fácil e seguro às mensagens de voz, via interface WEB ou telefone.

2.1.4 Fax Server

O Fax Server proporciona funcionalidades modernas e integradas para o envio e recebimento de faxes, incluindo:

- Integração com servidores de e-mail, oferecendo o recurso de e-mail to fax e fax to e-mail.
- Solução confiável e segura, que elimina a necessidade de hardware dedicado para gestão de faxes.
- Simplificação do processo de envio e recebimento, utilizando canais de comunicação já existentes.

2.2 Smartspace Collab

O Smartspace Collab é uma plataforma de Comunicações Unificadas e Colaboração da Smartspace, projetada para facilitar a comunicação integrada entre equipes e aumentar a produtividade organizacional. A solução reúne em uma única interface recursos avançados de voz, vídeo, chat, compartilhamento de tela, envio de arquivos e outras ferramentas essenciais para o trabalho colaborativo em tempo real.

Essa plataforma se destaca por sua flexibilidade e inovação, oferecendo suporte a diferentes dispositivos e garantindo uma experiência contínua e integrada para usuários em qualquer ambiente de trabalho, seja remoto, híbrido ou presencial.

2.2.1 Smartspace Communication Server

O Smartspace Communication Server é o núcleo central da plataforma de comunicações unificadas e colaboração. Ele é responsável por:

- Registro e gerenciamento de usuários, garantindo alta disponibilidade e eficiência nas comunicações.
- Controle de sessões de voz, vídeo e mensagens instantâneas.
- Integração completa com os demais módulos, permitindo uma experiência de uso integrada e sem interrupções.
- Suporte avançado para escalabilidade e segurança, adaptando-se perfeitamente a empresas de diferentes tamanhos e setores.

2.2.2 Smartspace IM Server

O Smartspace IM Server é um servidor de mensagens instantâneas (Instant Messaging) baseado no protocolo XMPP, totalmente integrado ao Smartspace Communication Server. Ele oferece:

- Comunicação fluida e em tempo real, com suporte a voz, vídeo, chat e compartilhamento de tela e arquivos.
- Ferramentas robustas de colaboração, que permitem a criação de grupos de trabalho e canais dedicados para diferentes projetos.
- Compatibilidade com diferentes dispositivos, garantindo conectividade contínua e acesso remoto.

2.2.3 Smartspace Squad

O Smartspace Squad é o cliente de comunicações unificadas e colaboração da plataforma. Intuitivo e poderoso, ele pode ser acessado por:

- Smartphones e tablets (iOS e Android), permitindo mobilidade total.
- Desktops e notebooks, através de navegadores web com tecnologia WebRTC.
- Recursos avançados que incluem:
    - Chamadas de voz e vídeo em alta definição.
    - Compartilhamento de tela e arquivos, ideal para apresentações e reuniões remotas.
    - Integração com ferramentas corporativas, ampliando as possibilidades de colaboração.

2.3 Smartspace Contact Center

O Smartspace Contact Center é uma plataforma omnichannel completa, desenvolvida para atender às demandas de comunicação e atendimento de contact centers modernos. Com um conjunto integrado de módulos avançados, a solução é projetada para proporcionar uma experiência excepcional ao cliente, aumentar a eficiência operacional e atender com excelência a múltiplos canais de interação.

Os principais diferenciais do Smartspace Contact Center incluem escalabilidade, flexibilidade e integração com diversas tecnologias, tornando-se uma solução ideal para empresas que buscam excelência em suas operações de atendimento.

2.3.1 Smartspace Metrics

O Smartspace Metrics é um serviço avançado de gerenciamento e controle do call center, permitindo:

- Monitoramento em tempo real de KPIs e métricas operacionais.
- Geração de relatórios detalhados, essenciais para análises estratégicas e tomada de decisões baseadas em dados.
- Suporte à personalização de dashboards para atender diferentes níveis de acesso e necessidades específicas.

2.3.2 Smartspace IVR Server

O Smartspace IVR Server é o serviço de URA (Unidade de Resposta Audível) que garante interações automatizadas, personalizadas e altamente eficientes. Com suporte à integração de tecnologias avançadas, como Inteligência Artificial, este módulo potencializa as operações de atendimento automatizado, permitindo a criação de voicebots inteligentes. Principais recursos incluem:

- Suporte ao padrão VXML, possibilitando a configuração de fluxos dinâmicos e personalizados de atendimento.
- Uso de IA para voicebots, permitindo interações mais naturais e contextualizadas com os clientes, otimizando processos e aumentando a taxa de resolução no primeiro contato.
- Integração com bases de dados, webservices e softwares de terceiros, garantindo comunicação fluida e adaptável às necessidades do negócio.
- Experiências avançadas de autoatendimento, que reduzem significativamente o tempo de espera e melhoram a satisfação do cliente.

2.3.3 Smartspace Record

O Smartspace Record é um módulo de gravação robusto e eficiente, projetado para capturar todas as chamadas da plataforma com alta confiabilidade. Principais benefícios:

- Funcionamento sem necessidade de espelhamento de portas de switch ou técnicas de gravação passiva.
- Armazenamento seguro das gravações, garantindo conformidade com regulamentações de privacidade e auditoria.
- Acesso fácil e rápido às gravações por meio de uma interface intuitiva, com recursos avançados de pesquisa e reprodução.

2.4 SMARTSPACE Manager/Monit

O Smartspace Manager/Monit é um serviço avançado de gestão e monitoramento da plataforma Smartspace e outros elementos de rede, projetado para oferecer visibilidade em tempo real, controle centralizado e gestão proativa dos recursos do sistema. Com suporte a protocolos como SNMP e ferramentas de análise avançada, o Manager/Monit é essencial para garantir a estabilidade, a eficiência e a confiabilidade de toda a infraestrutura.

Principais Funcionalidades:

- **Monitoramento em Tempo Real:** O sistema identifica e reporta ocorrências de falhas imediatamente, permitindo ações rápidas e precisas para minimizar impactos.
- **Gestão de Falhas:** As falhas são classificadas por categorias e priorizadas de acordo com sua urgência, garantindo que as mais críticas sejam tratadas com a máxima prioridade.
- **Interface de Gestão Intuitiva:** A plataforma oferece uma interface web amigável, que simplifica a visualização do status da infraestrutura e facilita a administração de recursos.
- **Sinalização por Rede TCP/IP:** Permite comunicação eficiente entre os componentes da solução, possibilitando a detecção e sinalização de problemas em múltiplos pontos.

Benefícios:

1. **Proatividade Operacional:** Com um sistema de alertas configurável, o SMARTSPACE Manager/Monit permite que equipes de TI atuem de forma proativa, evitando indisponibilidades e melhorando a experiência do cliente.
2. **Alta Confiabilidade:** A capacidade de monitorar e sinalizar falhas em tempo real reduz significativamente o tempo de inatividade, garantindo que os serviços essenciais estejam sempre disponíveis.
3. **Escalabilidade:** O sistema é preparado para gerenciar tanto ambientes compactos quanto infraestruturas corporativas de grande porte, adaptando-se às necessidades de crescimento da organização.

Casos de Uso:

- **Gerenciamento de Multi-Sites:** Ideal para empresas com operações distribuídas, permitindo o monitoramento centralizado de todos os sites.
- **Suporte a Protocolos Padrão:** A compatibilidade com SNMP e outros padrões facilita a integração com ferramentas de mercado e soluções de terceiros.
- **Gestão Baseada em Dados:** Relatórios detalhados sobre o desempenho da infraestrutura ajudam na tomada de decisões estratégicas e no planejamento de recursos.

2.5 **TARIF** – Sistema de Tarifação e Gestão de Telecom

O TARIF é uma solução robusta e completa de bilhetagem e tarifação telefônica, projetada para oferecer às empresas controle total sobre os custos de telecomunicações. Com uma interface 100% WEB, o sistema proporciona facilidade, agilidade e precisão na administração de recursos e na gestão financeira da plataforma de telefonia.

Principais Funcionalidades:

- **Bilhetagem Automática:** Registra e processa informações detalhadas sobre as chamadas realizadas, recebidas e internas, permitindo uma análise precisa dos custos de telecom.
- **Categorização de Custos:** Agrupamento por departamentos, projetos ou unidades organizacionais, facilitando a alocação de despesas e o planejamento orçamentário.
- **Geração de Relatórios Personalizados:** Oferece relatórios detalhados e gráficos que auxiliam na identificação de tendências de uso, consumo anômalo ou oportunidades de otimização.

- **Gestão de Tarifas:** Permite a configuração de tabelas de tarifas por operadora, horários e tipos de chamadas, garantindo total aderência às regras e políticas corporativas.
- **Monitoramento em Tempo Real:** Acompanha o uso de telecomunicações em tempo real, proporcionando visibilidade imediata para ajustes ou ações corretivas.

Benefícios:

- **Otimização de Custos:** Identifica desperdícios e oportunidades de economia, promovendo uma gestão mais eficiente dos recursos de telecom.
- **Transparência Operacional:** Oferece visibilidade completa dos custos, aumentando a transparência e facilitando auditorias internas e externas.
- **Facilidade de Uso:** Com uma interface web intuitiva, o TARIF simplifica o acesso e a navegação, permitindo que usuários de diferentes níveis de experiência utilizem a solução com facilidade.
- **Escalabilidade e Flexibilidade:** Ideal para empresas de todos os tamanhos, o sistema se adapta facilmente a diferentes demandas, desde pequenos escritórios até grandes corporações.

3 Características Gerais

A Plataforma Smartspace foi desenvolvida para atender às mais diversas demandas de comunicação corporativa, oferecendo uma solução escalável, confiável e altamente flexível. Sua arquitetura permite a criação de um cluster de servidores, garantindo máxima disponibilidade e desempenho, independentemente da quantidade de ramais e/ou usuários. Essa escalabilidade assegura que qualquer servidor defeituoso possa ser substituído sem impacto operacional, e novos servidores podem ser adicionados ao cluster para ampliar a capacidade de processamento. Todo o gerenciamento do cluster é realizado de forma unificada, com a plataforma tratando o cluster como um único sistema.

Além disso, a solução também está disponível para implementação em nuvem pública, permitindo que empresas usufruam de todos os recursos da plataforma com alta flexibilidade, redução de custos com infraestrutura física e acesso seguro a partir de qualquer localidade.

Funcionalidades e Recursos:

- **Gerenciamento centralizado** através de interface web de todos os recursos da plataforma.
- **Autenticação segura** com usuário e senha, com permissões de acesso configuradas conforme o perfil do usuário.
- **Compatibilidade com ambientes virtualizados**, como VMWare 6.x ou superior, Hyper-V e outras soluções de virtualização, sem restrições no uso de funcionalidades.
- **Compatibilidade com hardware hotswap:** O sistema pode ser instalado em hardware com suporte a hotswap, permitindo a ampliação ou substituição de placas de forma segura e eficiente, sem a necessidade de interromper os serviços em operação.
- **Oferta em ambiente multicloud:** A solução pode ser fornecida em ambientes multicloud com provedores públicos como AWS e OCI (Oracle Cloud Infrastructure), garantindo alta disponibilidade, escalabilidade e flexibilidade para atender às necessidades dos clientes.
- **Sistema multi-tenant:** O provisionamento e a configuração são realizados de maneira centralizada e unificada, garantindo eficiência e facilidade na gestão de múltiplas instâncias da solução.
- **Suporte à arquitetura orientada a serviços (SOA):** Baseada em XML, a solução permite maior flexibilidade e integração com diferentes sistemas.
- **Gerenciamento de multi-sites**, com administração centralizada de múltiplas localidades.
- **Alta disponibilidade com redundância ativo-ativo:** Todos os módulos da Plataforma SMARTSPACE oferecem suporte à operação em ativo-ativo, garantindo máxima disponibilidade e desempenho. Nesta modalidade, todos os servidores operam simultaneamente, proporcionando maior eficiência, resiliência e continuidade operacional, mesmo em cenários de falhas.
- Suporte a **banco de dados com replicação multi-master**, garantindo alta disponibilidade e integridade dos dados.
- Acesso seguro via HTTP ou HTTPS, com controle avançado de permissões.
- Suporte a uso de serviço HTTP e HTTPS para integrações;

- Suporte a acesso via SSH e SSH2.
- **Interface amigável** compatível com os principais navegadores, como Microsoft Edge, Mozilla Firefox, Google Chrome, Safari e Opera.
- **Gestão centralizada e intuitiva:** Permite a configuração, gerenciamento, administração e monitoramento de todos os recursos da solução por meio de uma interface gráfica web intuitiva e amigável, garantindo facilidade de uso e eficiência. Todas as operações podem ser realizadas sem a necessidade de interrupção dos serviços, assegurando continuidade operacional.
- **Recuperação segura de senhas** para usuários.
- Suporte a protocolos e padrões de mercado, incluindo **LDAP, Active Directory e SSO (Single Sign-On)**, com integração totalmente segura, sendo toda a configuração de integrações feita através de área específica na interface web.
- **Provisionamento centralizado e configuração unificada**, com suporte a múltiplos domínios LDAP e Active Directory.
- **Integração segura com LDAP e Active Directory:** Todas as versões de LDAP e AD são suportadas, utilizando conexões protegidas por SSL ou TLS. Opcionalmente, o sistema pode ser configurado para acesso sem SSL, dependendo dos requisitos do ambiente.
- **Importação em lote de usuários:** Permite a adição de múltiplos usuários de forma simultânea a partir dos servidores LDAP e AD, otimizando o processo de configuração inicial.
- **Redundância com múltiplos servidores e domínios LDAP/AD:** Possibilita a integração com múltiplos servidores e domínios LDAP ou AD, garantindo alta disponibilidade e confiabilidade.
- **Autenticação e controle de acesso baseados em LDAP:** Em conformidade com as especificações RFC 4510 e RFC 4511, assegurando padrões robustos e consistentes de segurança.
- **Autenticação em modo proxy:** O sistema não armazena as senhas dos usuários do LDAP, realizando a autenticação de forma segura e transparente através do modo proxy.
- **Importação completa de diretórios LDAP/AD:** Permite a criação de agendas telefônicas e internas da solução com dados detalhados, incluindo login, nome, sobrenome, ramal, telefone, e-mail, setor e localidade. Para agendas telefônicas, são utilizados campos como nome, sobrenome, ramal, local e telefone.
- **Configuração de sincronismo com LDAP/AD:** Possibilita a definição da periodicidade de sincronização, garantindo que os dados estejam sempre atualizados.
- **Compatibilidade com LDAPv3:** A solução oferece suporte integral ao protocolo LDAPv3, permitindo integrações modernas e alinhadas às necessidades empresariais.
- **Integração dinâmica com LDAP e Active Directory:** A integração permite que os parâmetros de pesquisa sejam configurados de forma dinâmica, proporcionando total transparência entre o Smartspace e as bases LDAP/AD.

- **Perfis de acesso baseados em grupos LDAP:** Suporte completo para perfis de acesso definidos com base nos grupos LDAP aos quais os usuários pertencem, abrangendo grupos Posix e não Posix.
- **Validação de grupos no login:** A validação do grupo LDAP ao qual o usuário pertence é realizada no momento do login, aumentando a segurança e a personalização do acesso.
- **Mapeamento de atributos personalizados:** Suporte ao mapeamento de atributos LDAP para personalizar o processo de sincronização e importação de dados, atendendo às necessidades específicas de cada cliente.
- **Integração com Microsoft Teams:** Permite a utilização da mesma base de credenciais e perfis do Microsoft Teams em soluções que possuem a integração habilitada, garantindo uma experiência integrada e contínua.
- **Gestão de usuários registrados:** O administrador tem acesso à visualização de todos os usuários registrados na solução, podendo gerenciar sessões de forma eficiente. É possível deslogar um único usuário, grupos de usuários ou todos os usuários simultaneamente, conforme necessário.
- **Controle de acesso por perfis:** Oferece um sistema robusto de controle de usuários, permitindo a configuração de múltiplos perfis de acesso, de acordo com as funções e responsabilidades de cada usuário.
- **Gestão avançada de usuários e perfis de acesso:** Permite o controle eficiente de usuários, com suporte a múltiplos perfis de acesso, adaptados às diferentes necessidades e responsabilidades dentro da solução.
- **Consulta e edição de dados de usuários:** Proporciona ferramentas práticas para visualizar e editar informações dos usuários de forma rápida e segura, garantindo uma gestão centralizada.
- **Criação de perfis personalizados:** Oferece a possibilidade de configurar perfis de acesso detalhados, assegurando que cada usuário tenha acesso apenas aos recursos e funcionalidades designados ao seu perfil.
- **Gestão robusta de acesso por perfis:** Oferece controle detalhado de acesso, permitindo a criação de perfis de usuários sem limitações quanto ao número de perfis cadastrados ou de usuários associados a cada perfil.
- **Gestão de perfis de acesso personalizados:** Permite o gerenciamento completo de perfis de acesso para todos os módulos da solução, incluindo criação, edição e exclusão. A criação de perfis é altamente flexível, permitindo configurar níveis específicos de acesso, como somente leitura, leitura para determinados módulos, edição ou exclusão em outros, adaptando-se às necessidades organizacionais.
- **Perfis de acesso para múltiplos sites:** Suporte à definição de perfis que abrangem todos os sites gerenciados ou que se aplicam a um ou mais sites específicos, proporcionando controle granular e eficiente.
- **Interface web para configurações personalizadas:** O sistema disponibiliza uma interface web que permite ao usuário realizar configurações do próprio ramal, e outros módulos do sistema, de forma simples e intuitiva. As funcionalidades incluem:
    - Troca de senha e alteração do idioma.
    - Ativação/desativação do voicemail e reprodução de mensagens.
    - Consulta ao CDR das chamadas realizadas e recebidas.

- Configuração de teclas de discagem rápida, grupos de transbordo, captura de chamadas, espera (hold) e outras funções do telefone.
- Ativação/desativação de recursos como desvios, siga-me, discagem rápida, não perturbe e cadeado eletrônico.
- Personalização de teclas do ramal, papel de parede e toque de chamada.

- **Acesso baseado em perfis:** Os usuários têm acesso às configurações disponibilizadas conforme o perfil definido pelo administrador do sistema, garantindo controle e segurança nas permissões.
- **Política configurável de senhas:** Oferece uma política de senhas personalizável, permitindo definir o tamanho mínimo, a quantidade de números, caracteres especiais e letras maiúsculas exigidos, aumentando a segurança no acesso ao sistema.
- **Suporte a senhas robustas:** Permite a criação de senhas com até 30 caracteres alfanuméricos, garantindo maior proteção contra acessos não autorizados.
- **Criação flexível de nomes de usuários:** O sistema permite a criação de logins utilizando combinações de letras, números e caracteres especiais, com suporte a tamanhos ilimitados. Além disso, é possível configurar se o sistema será case sensitive ou não, oferecendo maior flexibilidade para atender às políticas de nomenclatura e segurança de cada organização.
- **Acesso simultâneo para administração:** Permite que múltiplos usuários acessem simultaneamente as ferramentas de administração, conforme as licenças fornecidas, garantindo agilidade na gestão da solução.
- **Licenciamento flexível e adaptável:** Todos os módulos da plataforma possuem licenciamento flexível, permitindo configurações personalizadas para atender às demandas específicas de cada projeto.
- **Gerenciamento centralizado de licenças:** O gerenciamento das licenças é realizado de forma centralizada. Em caso de falha de comunicação entre sites remotos e o servidor central de licenças, a solução assegura a continuidade operacional dos sites remotos sem perda de funcionalidades. Após o restabelecimento da conexão, o sistema sincroniza automaticamente as informações de licenciamento.
- **Controle de licença baseado em software:** O controle de licença é realizado exclusivamente por meio de software, eliminando a necessidade de dispositivos físicos conectados aos servidores.
- **Armazenamento seguro de informações críticas:** Todas as informações críticas da solução são armazenadas de forma criptografada, garantindo máxima segurança e conformidade com padrões internacionais. Além disso, os backups exportados também são protegidos com criptografia, assegurando a integridade dos dados durante o armazenamento e transporte.
- **Backup via rede LAN:** A solução permite a geração de backups completos de toda a plataforma por meio da rede LAN, facilitando o gerenciamento e a proteção dos dados de forma centralizada e eficiente.
- **Suporte total a QoS e VLANs**, garantindo qualidade de serviço e separação de redes de voz e dados.

- **Suporte avançado a QoS:** A solução oferece suporte completo aos padrões de Qualidade de Serviço (QoS), incluindo IEEE 802.1p, DSCP, DiffServ, CoS e Type of Service, garantindo priorização eficiente do tráfego de voz, vídeo e dados em redes IP. Isso assegura qualidade superior para comunicações em tempo real, mesmo em ambientes de rede com alto volume de tráfego.
- **Baseado em padrões de mercado:** A solução opera de forma transparente em infraestrutura de rede IP (LAN, MAN, WAN), sendo totalmente independente do fabricante da infraestrutura, o que garante flexibilidade e compatibilidade com diversas configurações de rede.
- **Suporte a tráfego VoIP em redes WAN:** Oferece suporte abrangente ao tráfego VoIP por meio de tecnologias variadas, como **Internet, Frame Relay, MPLS, Wireless**, entre outras, assegurando qualidade de comunicação em diferentes tipos de redes.
- **Centralização de troncos SIP:** Possui um recurso avançado de centralização e gerenciamento unificado de troncos SIP, simplificando a administração e otimizando o uso dos recursos de comunicação.
- **Gerenciamento de grupos de chamadas:** Permite a associação de ramais a grupos específicos, definindo estratégias de roteamento personalizadas e números dedicados para melhorar a eficiência das chamadas internas e externas.
- **Ferramenta de análise de sinalização:** Inclui suporte para análise de sinalização SIP, R2 e ISDN, proporcionando maior controle e diagnóstico detalhado das comunicações.
- **Monitoramento avançado de troncos E1 e SIP:** Oferece suporte ao monitoramento detalhado dos troncos E1 e SIP, permitindo o diagnóstico proativo de possíveis falhas. Alertas são gerados automaticamente na interface de gerenciamento e/ou enviados por e-mail, assegurando uma resposta rápida para a resolução de incidentes.
- **Monitoramento de recursos do servidor:** Realiza o acompanhamento contínuo do uso de CPU, memória e HD em todos os servidores da solução, garantindo visibilidade em tempo real e facilitando a identificação de possíveis gargalos ou problemas de desempenho.
- **Compatibilidade com protocolos SIP:** A solução IP é totalmente compatível com os protocolos SIP RFCs 3261, 3262, 3265, 3311, 3513 e 3842, garantindo interoperabilidade com sistemas e dispositivos que seguem os padrões globais.
- **Funções SIP avançadas:** Oferece suporte para atuar como SIP Registrar, Proxy, Location, Redirect e Presence Server, ampliando a flexibilidade e funcionalidade das comunicações baseadas em SIP.
- **Manipulação avançada de cabeçalhos SIP:** Oferece suporte à manipulação, normalização e gerenciamento de cabeçalhos SIP, permitindo a criação de parâmetros de busca personalizados e adaptáveis às necessidades específicas.
- **Normalização de cabeçalhos SIP:** Permite a normalização de qualquer cabeçalho SIP, garantindo conformidade e interoperabilidade em cenários complexos.

- **Criação de serviços e aplicações baseados em XML:** Suporte para desenvolvimento de serviços e aplicações utilizando XML, acessíveis por computadores ou aparelhos IP compatíveis, ampliando as possibilidades de personalização e integração.
- **Operação como B2BUA:** Funciona como um Back-to-Back User Agent (B2BUA), permitindo maior controle sobre as chamadas e comunicações estabelecidas na solução.
- **Suporte a chamadas de áudio e vídeo:** Possui compatibilidade para chamadas de áudio e vídeo entre múltiplos endpoints, incluindo ramais IP, softphones mobile ou desktop e qualquer dispositivo autenticado, oferecendo flexibilidade para diversos cenários de uso.
- **Compatibilidade com CODECs de áudio e vídeo:**
    - **Áudio:** Suporte aos CODECs Opus, G711a, G711u, GSM, iLBC, G.722 (G.722.1C), G729, G729A e G729AB, além de outros, como codec2, ulaw, alaw, gsm, g726 e variantes.
    - **Vídeo:** Compatível com CODECs como VP9, VP8, H.261, H.263, H.263p, H.264, H.265 e MPEG, garantindo alta qualidade e interoperabilidade para comunicações multimídia.
- **Transcoding entre CODECs:** Suporta transcoding entre qualquer um dos CODECs de áudio e vídeo compatíveis, permitindo maior flexibilidade na adaptação às capacidades dos dispositivos conectados.
- **Cancelamento de eco de alta qualidade:** Oferece suporte ao cancelamento de eco conforme os padrões G.165 e G.168, garantindo maior clareza nas comunicações de áudio, mesmo em ambientes com ruídos ou configurações de rede desafiadoras.
- **Compatibilidade com BFCP (Binary Floor Control Protocol):** A solução é compatível com o protocolo BFCP, permitindo o controle eficaz de apresentações e compartilhamento de mídia em sessões de conferência.
- **Conformidade com NGN da ITU-T:** Atende a todos os requisitos de camada de serviços de Next Generation Network (NGN) definidos pela ITU-T, assegurando interoperabilidade e alinhamento com os padrões internacionais para redes de próxima geração.
- **Ampliação de capacidade sem interrupções:** Permite a ampliação da capacidade do sistema por meio de atualização de licenças e/ou inclusão de novos equipamentos, sem a necessidade de substituir o hardware existente e sem interrupção dos serviços em operação.
- **Autenticação flexível de ramais:** Suporte para autenticação de ramal em múltiplos dispositivos, incluindo aparelhos IP, analógicos e Softphones, utilizando o mesmo número de ramal, garantindo flexibilidade e mobilidade para os usuários.
- **Conferência telefônica com continuidade:** Suporte para conferências realizadas diretamente pelo telefone, possibilitando que o usuário/ramal que iniciou a chamada se retire sem que a mesma seja finalizada.
- **Funcionalidade "não perturbe" (DND):** Configuração direta no aparelho para ativar ou desativar o recurso não perturbe, proporcionando maior controle ao usuário sobre sua disponibilidade.

- **Chamada em espera diretamente pelo aparelho:** Possibilita colocar chamadas em espera diretamente pelo aparelho telefônico, simplificando a gestão de chamadas e melhorando a experiência do usuário.
- **Liberação automática de linhas telefônicas:** A solução oferece suporte à liberação automática de linhas telefônicas em diferentes situações, como ao término de chamadas, quedas de ligação ou outros eventos que desconectem a chamada, garantindo a disponibilidade rápida dos recursos e a otimização do sistema.
- **Gravação de chamadas com player web integrado:** A solução permite a gravação de chamadas, com um player web nativo para reprodução direta, oferecendo praticidade e acessibilidade ao gerenciamento dos arquivos de áudio.
- **Integração com storages para backup:** Suporte à integração com diferentes sistemas de storages para backup das gravações, garantindo segurança e fácil acesso aos arquivos armazenados.
- **Módulo de URA com suporte avançado:** Gerenciamento completo de árvores de URA, com suporte a tecnologias como ASR (Automatic Speech Recognition) e TTS (Text-to-Speech), permitindo interações mais dinâmicas e automatizadas com os usuários.
- **Módulo para gerenciamento de Contact Center:** Disponibiliza recursos específicos para administração eficiente de operações de Contact Center, melhorando a experiência do cliente e a performance da equipe.
- **Módulo de tarifação e bilhetagem:** Suporte à coleta de bilhetes, tanto de servidores gerenciados pela Plataforma SMARTSPACE quanto de servidores externos, oferecendo controle detalhado e relatórios de uso.
- **Módulos desenvolvidos internamente com suporte completo:** Todos os módulos da plataforma, incluindo PABX, URA, RECORD, TARIF, METRICS, MANAGER/MONIT, CONFERENCE, DIALER, ANALYTICS, BI, FAX, VOICEMAIL, PANEL, SOFTPHONE, IM/PRESENCE e SIP SERVER, são desenvolvidos pelo time de Pesquisa, Desenvolvimento e Inovação (PDI) da Smartspace. Estes módulos possuem suporte completo, garantindo a continuidade e evolução da solução para os clientes.
- **Integração com soluções de mercado:** A plataforma permite integração com outras soluções de mercado por meio do protocolo SIP ou através de APIs de integração fornecidas, garantindo flexibilidade e interoperabilidade com sistemas diversos.
- **Linha de produtos Audiocodes no portfólio Smartspace:** Toda a linha de produtos da Audiocodes faz parte do portfólio da Smartspace, podendo ser comercializada como produtos Smartspace. Esses dispositivos são plenamente compatíveis, devidamente homologados e incluem modelos como MediaPack 1xx, MediaPack 2xx, Mediant 8xx, Mediant 1xxx, Mediant 2xxx, Mediant 3xxx, Mediant 4xxx, Mediant 9xxx, Mediant SE/VE, entre outros.
- **Linha de produtos Yealink no portfólio Smartspace:** Toda a linha de produtos da Yealink também integra o portfólio da Smartspace, podendo ser comercializada como produtos Smartspace. Os dispositivos são plenamente compatíveis e homologados, contando ainda com versões de firmware personalizadas e especialmente desenvolvidas para a Smartspace.

- **Provisionamento e gerenciamento de end-points de vídeo:** A solução permite o provisionamento, gerenciamento e utilização de end-points de vídeo que operem com os protocolos suportados pela plataforma, ampliando as possibilidades de comunicação audiovisual.
- **Pacote de sobrevivência Smartspace:** O pacote de sobrevivência pode ser comercializado em conjunto com os equipamentos Gateways Digivox/Audiocodes, incorporando todos os recursos da Plataforma SMARTSPACE, incluindo SBC e suporte à sobrevivência local para até 50.000 usuários.
- **Geração de relatórios abrangentes:** Permite a criação de relatórios detalhados para análise e monitoramento dos dados da solução, incluindo métricas operacionais e de desempenho.
- **Relatórios específicos para Contact Center:** Disponibiliza relatórios dedicados ao Contact Center, oferecendo insights sobre desempenho, atendimento e eficiência da operação.
- **Histórico completo de auditoria:** Registra todas as modificações feitas nas configurações dos módulos, incluindo relatórios de auditoria para alterações realizadas, tentativas de login (válidas e inválidas) e outras intervenções. O log de auditoria armazena todos os passos dos usuários por um período configurável, garantindo rastreabilidade e compliance.
- **Detalhamento de logs de auditoria:** Os logs incluem informações detalhadas como o usuário responsável, data e hora da intervenção, endereço IP, porta usada para acesso, estado do registro antes e depois da alteração, item modificado e outros dados relevantes.
- **Geração e armazenamento de logs para suporte:** Armazena logs de todos os componentes da plataforma, inclusive de gateways externos, facilitando o diagnóstico de problemas e o suporte técnico.
- **Sistema operacional robusto e banco de dados confiável:** Utiliza distribuições Linux como CentOS, Slackware, Debian, RHEL, Oracle Linux, Suse Linux, entre outras, combinadas com o SGBD PostgreSQL com replicação multi-master, garantindo alta disponibilidade e integridade dos dados.
- **Configuração de serviços por servidor:** Suporte para configuração de serviços essenciais como SMTP, SNMP, FTP, TFTP, DHCP, IP/máscara/gateway/DNS estático, NFS, NTP, NTPS, NTPD, entre outros, proporcionando flexibilidade e personalização.
- **Suporte a IPv4 e IPv6:** Todos os módulos da solução operam de forma transparente com os protocolos IPv4 e IPv6, garantindo compatibilidade com infraestruturas de rede modernas.
- **Documentação e suporte online:** Disponibiliza documentação e ajuda online em português do Brasil, facilitando a consulta e o aprendizado dos usuários e administradores.

4 Arquitetura

A Plataforma SMARTSPACE foi projetada com uma arquitetura modular. Os módulos podem operar de forma integrada em um único servidor para soluções de pequeno porte ou distribuídos em diversos servidores, com cada servidor desempenhando um papel específico, ideal para soluções de grande porte.

A arquitetura atual da plataforma utiliza um banco de dados centralizado para armazenar todas as configurações do sistema, eliminando a necessidade de alterações manuais em arquivos locais nos servidores. Cada servidor da solução (SIP Server, VoiceMail, Contact Center - Metrics, Record, URA, etc.) utiliza um cache de memória local contendo todas as informações necessárias para seu funcionamento.

O banco de dados da Plataforma SMARTSPACE oferece suporte à replicação multi-master, permitindo que os dados sejam sincronizados entre dois ou mais servidores de forma transparente. Essa replicação possibilita:

- Modificação simultânea dos dados em diferentes servidores, com sincronização automática.
- Escalabilidade e alta disponibilidade por meio de um cluster de banco de dados.
- Continuidade operacional, mesmo em casos de indisponibilidade de um ou mais servidores, com sincronização automática das configurações após a normalização dos serviços.

Benefícios da Arquitetura

- **Configuração centralizada:** Todas as configurações são armazenadas no banco de dados, facilitando backups e replicações com outros datacenters.
- **Sincronização automática:** Qualquer configuração realizada no sistema central é automaticamente enviada para todos os servidores, atualizando o cache local.
- **Consistência entre servidores:** Os servidores compartilham informações do mesmo banco de dados. Assim, mesmo que os ramais estejam registrados em servidores fisicamente diferentes, todos os servidores têm acesso ao registro dos ramais por meio da base de dados compartilhada.
- **Facilidade de escalabilidade:** Adicionar novos SIP Servers ou outros módulos ao cluster é simples e sem impacto nos servidores existentes. A plataforma possui uma interface intuitiva para cadastro e remoção de servidores ou módulos.
- **Gestão simplificada:** Proporciona maior escalabilidade e eficiência na administração da Plataforma SMARTSPACE, reduzindo complexidades operacionais e otimizando os recursos disponíveis.

4.1 Alta Disponibilidade e Redundância

A Plataforma SMARTSPACE foi projetada para oferecer máxima disponibilidade e confiabilidade, atendendo desde soluções de pequeno porte até projetos de grande escala.

- **Modularidade e flexibilidade:** A arquitetura modular da plataforma facilita a implantação em diversas topologias, garantindo que os requisitos de disponibilidade sejam atendidos nos mais variados tipos de projetos.
- **Suporte a diferentes modos de redundância:** Todos os módulos da plataforma são compatíveis com as modalidades de redundância ativo/standby e ativo/ativo (hot-standby), dependendo da arquitetura implementada. Isso permite maior flexibilidade para adaptar a solução às necessidades específicas do cliente.
- **Replicação multi-master:** A plataforma suporta replicação multi-master das bases de dados, garantindo que os sites possam operar de maneira totalmente independente, mantendo todas as funcionalidades mesmo em cenários de perda de conectividade entre os locais.
- **Configurações centralizadas e sincronizadas:** Todas as configurações são armazenadas no banco de dados, assegurando que todos os elementos da solução estejam sempre atualizados, sem a necessidade de intervenções manuais ou execução de comandos para replicação.
- **Sincronização automática pós-indisponibilidade:** Em casos de falhas ou desconexões, os dados são sincronizados automaticamente entre os servidores redundantes assim que a conectividade é restabelecida, garantindo a continuidade operacional sem perda de informações.
- **Disponibilidade em nuvem pública com arquitetura multicloud:** A solução também pode ser disponibilizada em infraestrutura de nuvem pública utilizando provedores como AWS e Oracle Cloud Infrastructure (OCI). Essa arquitetura multicloud oferece escalabilidade, redundância geográfica e maior resiliência contra falhas, atendendo às necessidades de ambientes corporativos dinâmicos e distribuídos.

Essa abordagem robusta reforça o compromisso da Plataforma SMARTSPACE com alta disponibilidade, escalabilidade e eficiência operacional, oferecendo uma solução confiável para os mais exigentes ambientes corporativos.

4.1.1 Especificações técnicas

- **Redundância e failover com múltiplos servidores:** Suporte à implementação de soluções de alta disponibilidade, com múltiplos servidores localizados no mesmo site ou em sites remotos. Isso possibilita configurações de redundância local combinada com redundância remota, garantindo maior confiabilidade.
- **Topologia com redundância intra e inter site:** Permite a configuração de dois servidores redundantes dentro de um mesmo datacenter e servidores adicionais em outro datacenter remoto.
    - **Funcionamento em falhas:** Em caso de falha de um servidor no Datacenter 1, outro servidor redundante no mesmo datacenter assume automaticamente todas as funções de forma transparente e sem interrupção das chamadas em andamento. Caso ocorra uma falha adicional no servidor redundante, os servidores no Datacenter 2 assumem todas as operações de forma automática, mantendo a continuidade dos serviços sem perda de funcionalidades.

- **Recuperação automática:** O retorno dos serviços aos servidores originais ocorre automaticamente quando os servidores recuperam sua funcionalidade, garantindo a retomada suave das operações. Esses comportamentos podem ser ajustados conforme os requisitos específicos de cada projeto.

- **Sobrevivência local para sites menores:** Para projetos de grande porte, a solução suporta redundância/sobrevivência local em sites menores, permitindo que esses locais continuem operando de forma independente e sem perda de funcionalidades, mesmo na indisponibilidade dos datacenters primário e secundário.
- **Cluster escalável e balanceamento de carga:** Suporte à montagem de clusters com dois ou mais servidores para soluções de grande porte. O cluster opera em modos como ativo/standby, ativo/hot-standby ou ativo/ativo, com balanceamento de carga entre os servidores do cluster. Essa arquitetura distribui a autenticação dos usuários entre servidores localizados em diferentes localidades, oferecendo alta escalabilidade e desempenho.
- **Inicialização e sincronização automática de serviços:** A solução suporta a inicialização e sincronização automática de todos os serviços entre os clusters, mesmo após eventos de desligamento. Não é necessária nenhuma intervenção manual para reestabelecer os serviços.
- **Replicação automática entre localidades:** Os clusters são replicados automaticamente entre diferentes localidades, permitindo que os usuários utilizem qualquer uma delas para realizar login e acessar os recursos de forma transparente.
- **Sincronização pós-indisponibilidade:** Os servidores e configurações são sincronizados automaticamente entre os componentes da solução após eventos de parada ou indisponibilidade. Ao restabelecer a conexão, todos os dados são sincronizados de maneira automática e transparente.
- **Operação contínua durante indisponibilidades:** Em casos de indisponibilidade, o sistema continua operando com 100% das suas funcionalidades, possibilitando que administradores e usuários realizem configurações diretamente pela interface de gerência. Ao reconectar, o sistema sincroniza os dados de forma automática.
- **Redundância total dos módulos:** Todos os módulos da Plataforma SMARTSPACE possuem suporte a redundância, garantindo alta disponibilidade em todos os componentes.
- **Alta disponibilidade em diferentes modelos:** Recursos de alta disponibilidade, como redundância ativo-ativo e disaster recovery, estão disponíveis tanto em modelo on-premises quanto em arquitetura de nuvem pública, com entrega por parceiros como AWS e Azure, garantindo redundância em zonas distintas.
- **Continuidade de gravações durante migração:** Durante a migração para um servidor redundante, a solução mantém a gravação de chamadas ativas, sem perda de dados ou informações de busca no banco de dados.
- **Redundância local e geográfica:** Os clusters são compostos por dois ou mais servidores, permitindo redundância tanto local quanto geográfica. Em caso de falha de um servidor, os demais assumem automaticamente todas as funções, sem interrupção de chamadas em andamento ou perda de funcionalidades.

- **Suporte ao balanceamento de carga:** A solução inclui suporte a balanceamento de carga, distribuindo eficientemente as operações entre os servidores do cluster.
- **Alta disponibilidade garantida:** A solução assegura um índice de disponibilidade de 99,999%, alcançado por meio dos robustos recursos de redundância de software da Plataforma SMARTSPACE e dos hardwares especializados ofertados.
- **Criptografia avançada:** Suporte nativo à criptografia de sinalização e mídia utilizando DTLS/TLS e SRTP, garantindo segurança e proteção para todos os dados transmitidos.
- **Endereço IP Virtual (VIP):** A solução possui suporte nativo a VIP (Virtual IP Address) ou IP flutuante, utilizando o mecanismo Heartbeat. Além disso, permite a configuração de outros serviços redundantes com base no Heartbeat, oferecendo maior resiliência e continuidade operacional.
- **Fail-over automático com DNS-SRV:** Suporte à solução DNS-SRV, permitindo fail-over automático em caso de falha do servidor onde o endpoint está autenticado. Essa funcionalidade, combinada com endpoints SIP compatíveis, possibilita a montagem de uma estrutura de redundância escalável com múltiplos servidores, definindo a sequência de transbordo de autenticação à medida que os servidores enfrentam falhas.
- **Registro simultâneo de ramais:** Os ramais podem ser registrados simultaneamente nos servidores primário e secundário, garantindo continuidade das operações em cenários de indisponibilidade.
- **Redundância física de rede:** A solução permite a agregação de interfaces de rede, garantindo redundância física das portas de rede e maior confiabilidade da conectividade.
- A plataforma Smartspace suporta autenticação unificada por meio de Single Sign-On (SSO), permitindo que o usuário utilize uma única identidade corporativa para acessar os serviços autorizados. Após a autenticação inicial, o acesso aos diferentes módulos ocorre sem a necessidade de nova digitação de senha, respeitando as políticas de segurança, perfis e permissões definidos pela CONTRATANTE.
- A integração com diretórios corporativos pode ser realizada por meio de LDAP e Microsoft Active Directory, possibilitando a centralização da autenticação e a utilização das credenciais já mantidas pela CONTRATANTE. A implementação considera as políticas de segurança e governança estabelecidas pela ATI, sem exigir a manutenção de senhas independentes na plataforma.
- A sinalização SIP contempla mecanismos voltados à privacidade e à proteção da identidade dos usuários, incluindo tratamento de informações de origem, identidade declarada e encaminhamento de chamadas em ambientes confiáveis. Esses recursos permitem preservar ou apresentar a identificação conforme as regras de segurança, roteamento e interconexão estabelecidas.
- A plataforma realiza o tratamento dos cabeçalhos SIP utilizados para informar os motivos de encerramento, rejeição, cancelamento ou redirecionamento de chamadas. Essas informações podem apoiar a interoperabilidade entre sistemas, a análise de falhas e o diagnóstico operacional dos serviços de voz.
- As operações de transferência de chamadas são suportadas por meio dos mecanismos SIP REFER, Replaces e Referred-By, abrangendo transferências cegas e assistidas. A solução preserva as informações necessárias sobre a sessão original, o destino e a origem da transferência, conforme as políticas definidas para o serviço.
- Os mecanismos de publicação e acompanhamento de presença permitem disponibilizar informações de estado dos usuários e terminais, como disponibilidade, ocupação e atividade. A aplicação desses recursos depende da configuração dos serviços, dos terminais utilizados e da interoperabilidade com as plataformas integradas.

- O tratamento do cabeçalho SIP Join possibilita associar uma nova sessão a um diálogo já existente, apoiando funcionalidades de conferência, inclusão de participantes e outras interações controladas entre chamadas.
- A utilização de Session Timers permite monitorar e atualizar periodicamente as sessões SIP, identificando chamadas desconectadas de forma anormal e liberando os respectivos recursos. Os intervalos e critérios de atualização podem ser ajustados de acordo com as características da rede e dos elementos integrados.
- A plataforma contempla o uso de tipos alternativos de endereçamento de rede em sessões SIP e SDP, inclusive em ambientes IPv4 e IPv6. Esse tratamento contribui para a interoperabilidade durante cenários de transição, coexistência ou escolha dinâmica do endereço utilizado para sinalização e mídia.
- A comunicação segura pode ser estabelecida mediante SIP sobre TLS e SIPS, protegendo a sinalização entre os componentes autorizados. A reutilização controlada de conexões seguras contribui para a eficiência operacional, redução de novas negociações de transporte e manutenção da comunicação em ambientes de alta demanda.
- Os mecanismos de redirecionamento e desvio de chamadas preservam as informações relacionadas à numeração original e aos destinos intermediários. Isso permite aplicar corretamente regras de encaminhamento, tarifação, identificação, roteamento e tratamento por URAs ou filas de atendimento.
- A solução contempla o tratamento atualizado de identidade assertiva em redes SIP confiáveis, possibilitando a utilização controlada de informações como P-Asserted-Identity e P-Preferred-Identity. O uso desses cabeçalhos observa as relações de confiança estabelecidas entre os elementos da rede.
- A compatibilidade com IPv6 inclui o correto tratamento de endereços, sintaxe, comparação de URIs e parâmetros utilizados na sinalização SIP. A funcionalidade permite a operação em ambientes IPv6 ou de coexistência com IPv4, conforme a infraestrutura disponibilizada.
- O suporte a SIP INFO permite o transporte de informações adicionais durante uma sessão estabelecida, de acordo com os pacotes negociados entre os elementos integrados. Esse recurso pode ser utilizado em funcionalidades complementares, desde que suportadas pelos sistemas participantes da comunicação.
- A plataforma contempla o uso de RTP e RTCP para transporte e controle dos fluxos de mídia, incluindo a negociação dos respectivos parâmetros por meio do SDP. As informações de RTCP apoiam o acompanhamento de qualidade, perda de pacotes, variação de atraso e demais indicadores relevantes à operação de voz.
- Os parâmetros de largura de banda podem ser sinalizados por meio do SDP, permitindo que os elementos envolvidos considerem as necessidades de cada fluxo de mídia. Esse recurso contribui para a interoperabilidade e para a aplicação de políticas de capacidade e qualidade de serviço.
- A solução suporta a negociação de mecanismos de proteção da mídia por meio do SDP, incluindo descrições de segurança associadas a fluxos SRTP. Dessa forma, podem ser estabelecidos parâmetros de criptografia e autenticação de mídia entre componentes compatíveis e devidamente configurados.
- A indicação de mensagem em espera permite informar aos usuários e terminais sobre a existência de novas mensagens na caixa postal. A sinalização pode ser apresentada por meio de indicador visual, notificação no terminal ou recurso equivalente disponibilizado pelo dispositivo utilizado.
- O monitoramento de diálogos SIP possibilita acompanhar o estado das chamadas associadas a usuários, ramais ou recursos monitorados. Essa funcionalidade pode ser utilizada em recursos como presença telefônica, teclas de acompanhamento, supervisão de ramais e indicação de chamadas em andamento.
- Os eventos de conferência permitem acompanhar o estado da sessão e de seus participantes, conforme os recursos habilitados e a compatibilidade dos elementos integrados. A plataforma também trata informações e estatísticas consolidadas de RTCP, contribuindo para o monitoramento da qualidade das comunicações.
- A portabilidade e a migração da numeração telefônica podem ser conduzidas de forma planejada, preservando o plano de numeração utilizado pela CONTRATANTE. O processo contempla levantamento da base, validação de titularidade, preparação de rotas, agendamento das janelas e acompanhamento da ativação, em conformidade com a regulamentação aplicável da ANATEL.
- Durante a transição, podem ser adotados procedimentos de contingência, testes de chamadas e validações de entrada e saída, com o objetivo de reduzir impactos sobre os usuários. Após a ativação, são verificados

aspectos como apresentação do número, encaminhamentos, chamadas locais e de longa distância, integração com URAs, filas e demais funcionalidades contratadas.

- A operação dos números migrados permanece integrada à infraestrutura de comunicação fornecida, preservando as regras de roteamento, perfis de usuários e serviços associados. O processo inclui acompanhamento técnico da estabilização para identificação e tratamento de eventuais inconsistências de interconexão.
- A plataforma Smartspace permite a integração com serviços de Discagem Direta Gratuita, incluindo numerações com prefixo 0800 e tarifação reversa. As chamadas recebidas podem ser direcionadas para URAs, filas, grupos de atendimento, agentes ou destinos previamente definidos.
- O tratamento das chamadas 0800 pode considerar origem, horário, disponibilidade dos atendentes, prioridade, transbordo e regras específicas de distribuição. Também podem ser disponibilizados registros operacionais e informações de chamadas para acompanhamento do serviço, observadas as funcionalidades e integrações incluídas no escopo contratado.
- Como referência de interoperabilidade, a plataforma possui suporte às RFCs aplicáveis à sinalização, identidade, privacidade, transferência, presença, segurança e gerenciamento de sessões SIP: RFC 3323, RFC 3325, RFC 3326, RFC 3515, RFC 3891, RFC 3892, RFC 3903, RFC 3911, RFC 4028, RFC 4092, RFC 5630, RFC 5806, RFC 5876, RFC 5923, RFC 5954 e RFC 6086.
- Para negociação, transporte, controle e proteção dos fluxos de mídia, a solução também contempla suporte às RFCs relacionadas a SDP, RTP, RTCP, SRTP, eventos e conferência: RFC 3605, RFC 3890, RFC 4091, RFC 4567, RFC 4568, RFC 3842, RFC 4235, RFC 4575 e RFC 6035.
- O suporte a essas especificações assegura a interoperabilidade da Plataforma Smartspace com operadoras, SBCs, terminais SIP, sistemas de comunicação unificada e demais componentes compatíveis, observadas as funcionalidades habilitadas, as versões de software e os parâmetros técnicos definidos para cada integração.

- A plataforma permite aplicar políticas de aceitação ou rejeição de chamadas com base nas informações de origem recebidas da rede pública. Dessa forma, chamadas originadas por telefones públicos podem ser identificadas e bloqueadas conforme as regras de segurança e atendimento definidas pela CONTRATANTE, desde que a operadora entregue corretamente os respectivos indicadores de origem.
- A solução suporta o encaminhamento de chamadas destinadas ao Serviço Móvel Pessoal nas modalidades VC2 e VC3, contemplando comunicações móveis inter-regionais e de longa distância nacional. A classificação, o completamento e a tarifação das chamadas observam o plano contratado com a operadora e a regulamentação aplicável da ANATEL.
- A arquitetura contempla mecanismos de NAT Traversal para permitir o estabelecimento da sinalização e dos fluxos de mídia em redes com tradução de endereços e políticas de firewall. O suporte a STUN, TURN e ICE possibilita identificar endereços públicos, selecionar rotas de conectividade e utilizar retransmissão de mídia quando não for viável estabelecer uma comunicação direta entre os participantes.
- A plataforma permite a marcação e a preservação dos parâmetros de qualidade de serviço nos pacotes de sinalização e mídia, incluindo ToS e DSCP. As classes de tráfego podem ser configuradas para priorizar voz e vídeo sobre aplicações menos sensíveis a atraso, observadas as políticas de QoS implementadas na rede da CONTRATANTE e nos elementos intermediários.
- O SBC atua como elemento de proteção de borda, aplicando controle de acesso, validação de sessões, limitação de tráfego e identificação de comportamentos anômalos. Esses mecanismos contribuem para a mitigação de ataques DoS e DDoS, falsificação de origem, mensagens SIP malformadas, manipulação de cabeçalhos, tentativas de registro indevidas e demais ameaças direcionadas aos serviços de comunicação.
- A arquitetura contempla funções de firewall SIP integradas ao SBC, com inspeção e normalização da sinalização, aplicação de regras por endereço, domínio, usuário, tronco e interconexão, além do bloqueio de origens não autorizadas. As políticas podem ser ajustadas conforme o perfil de segurança e as relações de confiança estabelecidas para cada integração.

- A solução suporta o recebimento e o encaminhamento de entroncamentos provenientes de operadoras de telecomunicações, centrais de atendimento, plataformas de colaboração e outros ambientes SIP. A interconexão pode ser distribuída entre pontos de voz geograficamente separados no Brasil, hospedados em datacenters de alta disponibilidade, permitindo redundância, continuidade operacional e alternativas de roteamento.
- O SBC corporativo realiza a proteção, o controle e a normalização do tráfego de sinalização e mídia. Entre suas funções estão o ocultamento da topologia interna, controle de sessões, interoperabilidade SIP, tratamento de NAT, aplicação de políticas de segurança e proteção dos fluxos de voz e vídeo.
- O SmartBot Pro contempla recursos de reconhecimento automático de fala, síntese de voz e processamento de linguagem natural. A integração com mecanismos de IA Generativa permite interpretar o contexto da conversa, compreender solicitações em linguagem natural, produzir respostas contextualizadas e direcionar o atendimento automatizado ou humano de acordo com as regras definidas para cada jornada.
- Os processos de gestão do ciclo de vida dos ativos contemplam procedimentos de reutilização, transferência, descarte e alienação segura de mídias e equipamentos. O tratamento considera a classificação das informações, a eliminação segura dos dados e a manutenção das evidências aplicáveis, em alinhamento aos controles de segurança da informação da ISO/IEC 27001:2022.
- A infraestrutura é submetida periodicamente a processos de identificação, análise e tratamento de vulnerabilidades. As atividades podem compreender varreduras automatizadas, avaliações técnicas, classificação por criticidade, definição de planos de correção e geração de evidências ou relatórios, conforme as condições de segurança, confidencialidade e governança estabelecidas contratualmente.
- O ambiente emprega mecanismos de prevenção, detecção e contenção de códigos maliciosos, associados a políticas de atualização, monitoramento de eventos e controle de acesso. A proteção é aplicada aos componentes pertinentes da infraestrutura, respeitando as características técnicas e as responsabilidades de cada camada do serviço.
- A arquitetura do SmartBot Pro permite expansão horizontal dos componentes de processamento e distribuição das requisições entre instâncias disponíveis. O ambiente pode ser dimensionado para processar, no mínimo, 100 usuários ou requisições por segundo, mantendo capacidade de crescimento conforme o volume de sessões, a complexidade dos fluxos e os critérios de desempenho definidos para o projeto.
- A plataforma suporta autenticação federada pelo protocolo OpenID Connect, permitindo integração com provedores corporativos de identidade. O usuário pode utilizar sua identidade institucional para acessar os serviços autorizados, enquanto a gestão de autenticação, políticas de acesso e ciclo de vida das credenciais permanece centralizada no provedor definido pela CONTRATANTE.
- O histórico do atendimento e o conteúdo das conversas podem ser disponibilizados ao cliente por meio eletrônico, conforme o canal e o fluxo configurados. O registro preserva informações como identificação do atendente, data, horário, protocolo e conteúdo da interação, proporcionando rastreabilidade e suporte aos processos de auditoria.
- A interface apresenta imediatamente ao usuário o conteúdo digitado, sem depender de processamento remoto para exibição dos caracteres. A troca das mensagens utiliza comunicação em tempo real, proporcionando fluidez às conversas entre cliente, atendente e demais participantes do atendimento.
- O SmartBot Pro utiliza processamento otimizado e componentes escaláveis para manter o tempo de resposta compatível com uma conversação natural. A latência efetiva pode ser monitorada durante a operação e depende também da conectividade, do canal utilizado, dos serviços externos integrados e da complexidade do processamento solicitado.
- Os dashboards e relatórios gerenciais podem apresentar informações por meio de gráficos de linhas, áreas, colunas, barras, pizza e demais modelos de visualização disponibilizados pelo mecanismo analítico. Quando previsto na configuração do ambiente, também podem ser utilizadas representações tridimensionais compatíveis com a ferramenta de Business Intelligence adotada.
- A autenticação centralizada pode ser realizada por meio de SAML 2.0 ou OpenID Connect, permitindo integrar os usuários da solução aos provedores de identidade homologados pela CONTRATANTE. O SSO pode

ser aplicado aos módulos habilitados, observando os perfis de acesso, atributos de identidade e políticas de segurança definidas para cada grupo de usuários.

- A geração de relatórios utiliza mecanismos controlados de consulta e processamento, permitindo acesso online, exportação e impressão das informações. A execução pode ser organizada de maneira assíncrona e com controle de recursos, evitando impacto significativo sobre os atendimentos, a sinalização e as demais atividades operacionais em produção.
- Os relatórios são administrados por interface Web unificada, por meio da qual usuários autorizados podem consultar, parametrizar, gerar e disponibilizar novos modelos. A entrada em produção de um relatório não exige a interrupção dos relatórios ativos nem dos serviços de atendimento.
- A plataforma disponibiliza relatórios relacionados a agentes, filas, campanhas, interações, canais e indicadores de desempenho. Os dados podem ser filtrados por período, operação, equipe, resultado e demais atributos disponíveis, respeitando os perfis de acesso e a abrangência de visualização de cada usuário.
- A sinalização SDP contempla os atributos necessários para a negociação de sessões de mídia protegidas e orientadas à conexão sobre TLS. A solução pode negociar parâmetros de transporte, identificação do certificado e proteção do canal, proporcionando confidencialidade e autenticação entre elementos compatíveis.
- O SBC realiza inspeção stateful das sessões, acompanhando a evolução dos diálogos SIP e mantendo informações sobre as conexões ativas. Esse controle permite validar se as mensagens recebidas pertencem a sessões legítimas, rejeitar tráfego incompatível com o estado esperado e liberar recursos após o encerramento da comunicação.
- As políticas de segurança seguem o princípio de permissão explícita, restringindo o tráfego aos protocolos, endereços, portas e aplicações necessários aos serviços de comunicação. Protocolos ou conexões não autorizados podem ser rejeitados antes de alcançar os componentes internos da plataforma.
- As políticas de acesso da borda SIP podem ser configuradas por faixas de endereços IP autorizadas. A aplicação dessas políticas por ramal ou tipo de dispositivo permite limitar, por exemplo, o registro de telefones institucionais às redes internas ou a outras redes previamente definidas.
- Tentativas de registro provenientes de origens fora das faixas autorizadas são bloqueadas conforme a política configurada. Os eventos de autenticação e bloqueio podem ser registrados para acompanhamento e auditoria.
- A proteção contra ameaças relacionadas à camada 2 é aplicada pela infraestrutura de rede e pelos controles do datacenter, abrangendo segmentação, proteção de tabelas de endereços, limitação de conexões, validação do tamanho dos pacotes e tratamento de timeouts. Esses controles atuam de maneira complementar às proteções de sinalização e mídia oferecidas pelo SBC.
- O ambiente possui mecanismos para identificação e bloqueio de tentativas de reconhecimento, varredura de portas e exploração sistemática de endereços ou serviços. Os eventos podem ser registrados e correlacionados para apoiar o monitoramento e o tratamento de comportamentos suspeitos.
- O controle de tráfego pode ser aplicado por usuário, endereço, tronco, domínio e interconexão. As políticas de rate limiting estabelecem limites para registros, tentativas de chamada, mensagens SIP e sessões simultâneas, reduzindo os efeitos de ataques de negação de serviço e evitando o consumo indevido dos recursos da plataforma.
- O SBC realiza inspeção configurável dos cabeçalhos e das informações transportadas na sinalização SIP, permitindo validar formato, conteúdo, sequência e consistência das mensagens. Quando atua como ponto de terminação ou controle da comunicação, a solução aplica as políticas de inspeção compatíveis com os protocolos utilizados e com o nível de criptografia adotado.
- Como referência técnica, os mecanismos de conectividade em ambientes com NAT, STUN, TURN e ICE são suportados conforme as RFCs 8489, 8656 e 8445. A priorização do tráfego por DSCP observa os princípios definidos nas RFCs 2474 e 4594.

- Os recursos de sinalização, privacidade, identidade e segurança SIP observam, entre outras especificações aplicáveis, as RFCs 3261, 3323, 3325, 3326, 3581, 4028, 4474, 5923 e 5630. Os mecanismos de SDP, transporte e proteção da mídia contemplam as RFCs 4566, 4145, 4572, 3711 e 4568.
- A integração por OpenID Connect segue a especificação OpenID Connect Core 1.0 e o OAuth 2.0, definido pela RFC 6749. A proteção da autenticação e das comunicações Web pode utilizar TLS conforme as RFCs 8446 e 8996, observadas as versões e políticas criptográficas habilitadas no ambiente.
- A arquitetura do SBC é dimensionada para executar inspeção, análise, normalização e bloqueio do tráfego sem introduzir atrasos perceptíveis nas comunicações. A capacidade de processamento considera o volume de sessões simultâneas, tentativas de chamadas por segundo, registros SIP, criptografia e demais funcionalidades de segurança previstas para o ambiente contratado.
- O SBC possui mecanismos de proteção contra avalanches e tempestades de registros SIP, controlando a quantidade de solicitações recebidas por usuário, endereço, domínio e intervalo de tempo. As requisições legítimas podem ser processadas progressivamente, evitando a sobrecarga do SBC e dos servidores de aplicação durante processos de recuperação, reinicialização de terminais ou restabelecimento massivo da conectividade.
- A gestão operacional das equipes contempla acompanhamento de escalas, produtividade, disponibilidade, desempenho individual e indicadores de qualidade. As funcionalidades avançadas de Workforce Management podem ser disponibilizadas por meio do módulo WFM integrado à Plataforma Smartspace, conforme a composição funcional estabelecida para o projeto.
- O copiloto de IA opera de forma contextual e integrada ao ambiente de atendimento, utilizando os dados autorizados da interação, o perfil do usuário e as bases de conhecimento disponibilizadas pela organização. O acesso às informações observa as permissões, políticas de segurança e critérios de governança definidos pela CONTRATANTE.
- Durante o atendimento, o assistente de IA pode apoiar o agente com sugestões de respostas, recuperação de informações, orientações operacionais e geração de resumos. As recomendações são apresentadas como apoio à decisão, permanecendo sob responsabilidade do atendente a validação e o envio das informações ao cliente.
- A arquitetura da plataforma permite a evolução para assistentes voltados às atividades administrativas, utilizando linguagem natural e APIs controladas. Funcionalidades como criação de usuários, filas ou políticas de roteamento podem ser incorporadas em roadmap, condicionadas a validações, permissões administrativas, registros de auditoria e mecanismos de confirmação antes da execução.
- Os recursos de IA podem operar integrados à experiência do Contact Center, preservando o contexto das interações e reduzindo a necessidade de alternância entre aplicações. A disponibilização das funcionalidades observa o escopo contratado, as políticas de uso da CONTRATANTE e a configuração dos modelos ou serviços cognitivos habilitados.
- Nas interações digitais, o histórico, as mensagens e o contexto do atendimento são preservados durante indisponibilidades temporárias, permitindo a retomada após o restabelecimento da comunicação. Nas chamadas de voz, os registros e dados do atendimento são mantidos, embora a sessão telefônica interrompida dependa do restabelecimento ou da realização de uma nova chamada.
- Os scripts de atendimento podem ser apresentados integralmente ou organizados em etapas guiadas. No formato de assistente visual, as próximas perguntas, orientações e campos são exibidos conforme as respostas anteriores, permitindo criar jornadas condicionais e direcionar o atendente durante a execução do processo.
- Os supervisores podem ser habilitados temporariamente para atuar como agentes e receber interações das filas durante períodos de maior demanda. Essa atuação respeita as habilidades, canais, filas, prioridades e permissões associadas ao perfil do supervisor.
- O comportamento das chamadas pode ser configurado conforme as regras operacionais estabelecidas pela CONTRATANTE, incluindo ações de manutenção, encerramento, transferência, retorno à fila ou

encaminhamento para outro destino. As permissões podem variar conforme o perfil do usuário, o tipo de atendimento e o estado da interação.

- O softphone permite utilizar os dispositivos de áudio disponíveis no computador ou equipamento móvel, incluindo alto-falantes, microfones e dispositivos Bluetooth compatíveis. A operação em modo viva-voz preserva a continuidade da chamada, observadas a qualidade da rede, as características do equipamento e a configuração dos recursos de áudio.
- A administração dos atendentes é realizada por interface gráfica Web, permitindo incluir, alterar, desabilitar e consultar usuários, estados e parâmetros operacionais. A execução dessas atividades é controlada por perfis de acesso e pode gerar registros de auditoria para identificação do administrador responsável pelas alterações.
- As funcionalidades de Workforce Management abrangem coleta de dados históricos, previsão de demanda, dimensionamento, criação de escalas, acompanhamento intradiário e análise de aderência. A integração com os dados operacionais da Plataforma Smartspace permite relacionar demanda, disponibilidade da equipe, níveis de serviço e resultados efetivamente alcançados.
- A gestão de escalas permite realizar alterações e trocas de turnos considerando habilidades, jornadas, tarefas, restrições legais e necessidades da operação. As solicitações podem seguir fluxos de proposta, aceite e aprovação, mantendo rastreabilidade das alterações realizadas.
- O acompanhamento intradiário permite comparar o planejamento com a situação efetiva da operação ao longo do dia. Diante de ausências, picos de demanda ou variações inesperadas, os gestores podem redistribuir recursos, ajustar atividades e adotar ações para preservar os níveis de serviço.
- O dimensionamento da força de trabalho considera o volume previsto, o tempo médio de atendimento, a ocupação desejada, as pausas e os objetivos de nível de serviço. A partir dessas informações, a solução auxilia na definição da quantidade adequada de atendentes por período, reduzindo situações de ociosidade ou insuficiência de capacidade.
- Os recursos analíticos permitem comparar o desempenho atual e histórico por atendente, equipe, unidade e visão corporativa. Os indicadores consolidados apoiam a identificação de tendências, desvios de produtividade, alterações no perfil da demanda e oportunidades de melhoria.
- A previsão de demanda utiliza dados históricos e parâmetros operacionais para estimar o comportamento futuro das interações. Podem ser consideradas sazonalidade, tendências, dias da semana, horários, campanhas e outros eventos relevantes para o planejamento dos recursos.
- A solução permite simular diferentes volumes de entrada, tempos de atendimento e níveis de disponibilidade da equipe. Os resultados demonstram os possíveis impactos sobre filas, ocupação, tempo de espera e nível de serviço, apoiando a seleção da estratégia operacional mais adequada.
- Os prognósticos podem abranger operações receptivas, ativas e canais digitais integrados à solução omnichannel. O tratamento considera as particularidades de cada canal, como simultaneidade das interações, tempo médio de atendimento, produtividade e habilidades requeridas.
- A aderência em tempo real permite comparar a escala planejada com as atividades efetivamente executadas pelos atendentes. Os gestores podem identificar atrasos, ausências, pausas não programadas ou desvios de atividade e adotar ações corretivas durante a própria jornada.
- Os resultados podem ser apresentados nas perspectivas planejada, em execução e realizada, permitindo acompanhar a evolução da operação em relação ao forecast e ao schedule. Essa comparação proporciona uma visão contínua da aderência, da capacidade disponível e do cumprimento das metas.
- As séries históricas de chamadas e interações podem ser analisadas em intervalos específicos para estimar volumes futuros. Com base nas projeções, a solução calcula a necessidade de recursos e auxilia na composição das escalas necessárias para alcançar os níveis de serviço estabelecidos.
- As simulações do tipo *what-if* permitem incluir eventos especiais, campanhas, feriados, indisponibilidades, alterações no tempo médio de atendimento e variações de demanda. A comparação entre cenários esperado, otimista e crítico facilita a preparação da operação para diferentes condições.

- Como referência técnica, a sinalização e o registro de usuários SIP observam a RFC 3261, enquanto os mecanismos de conexão persistente, recuperação e registro em ambientes distribuídos podem utilizar os princípios das RFCs 5626 e 5627. A proteção contra avalanches de registros é complementada por políticas próprias de rate limiting, controle de admissão e detecção de anomalias implementadas pelo SBC.
- A segurança das comunicações pode contemplar TLS conforme as RFCs 8446 e 8996, SIP sobre TLS e SIPS conforme as RFCs 3261 e 5630, além de SRTP conforme a RFC 3711. A qualidade e o monitoramento dos fluxos de mídia podem utilizar RTP e RTCP, definidos nas RFCs 3550 e 3611.
- As funcionalidades de gestão da força de trabalho utilizam métodos estatísticos de previsão, dimensionamento e análise de séries temporais, além de modelos de filas, como Erlang C, quando aplicáveis ao tipo de operação. Por não constituírem protocolos de comunicação, Forecasting, Scheduling e Adherence não possuem uma RFC específica.
- A utilização de IA pode ser governada por controles alinhados à ISO/IEC 42001, à ISO/IEC 23894 e às políticas de segurança da informação da ISO/IEC 27001:2022, contemplando gestão de riscos, controle de acesso, rastreabilidade e supervisão humana.
-
-
- Para operações novas que ainda não disponham de histórico próprio, o módulo WFM permite criar perfis iniciais de demanda utilizando parâmetros manuais, jornadas semelhantes ou padrões estáveis definidos pela equipe de planejamento. Esses modelos podem ser utilizados como referência temporária e aperfeiçoados à medida que os dados reais da nova operação sejam coletados.
- As curvas de previsão podem ser ajustadas manualmente por meio de interface gráfica, permitindo alterar os volumes estimados em intervalos específicos. Após a redefinição da curva, os novos valores são considerados nos cálculos de dimensionamento, ocupação, escala e nível de serviço.
- Os componentes de Forecasting, Scheduling, Intraday Management, Adherence e Workforce Analytics são disponibilizados como uma suíte integrada do mesmo fabricante do módulo WFM. A suíte se integra à Plataforma Smartspace por meio de APIs e conectores homologados, preservando a centralização dos dados operacionais e a experiência de gestão da solução ofertada.
- As interações realizadas pelo Assistente Virtual podem ser analisadas e qualificadas de acordo com critérios como intenção identificada, resposta apresentada, nível de confiança, conclusão da jornada, abandono, transbordo para atendimento humano e avaliação do usuário. Essas informações apoiam a curadoria e a evolução contínua da automação.
- As mensagens recebidas e as respectivas classificações podem ser acompanhadas por meio de indicadores analíticos. A evolução do assistente pode ser medida considerando volume de interações, taxa de reconhecimento, retenção no atendimento automatizado, intenções não identificadas, respostas sem resultado e recorrência de solicitações.
- A análise consolidada das conversas permite identificar lacunas de conteúdo, novas intenções, perguntas recorrentes, pontos de abandono e oportunidades de automação. Os insights gerados apoiam a priorização de melhorias nos fluxos, na base de conhecimento e nas integrações utilizadas pelo Assistente Virtual.
- O ambiente de curadoria permite validar, mapear, dividir, unir, reorganizar e remanejar intenções, entidades e conteúdos. Também contempla atividades de indexação, reindexação, revisão de respostas, tratamento de fluxos e representação textual dos assuntos reconhecidos pelo motor cognitivo.
- A plataforma permite construir e validar protótipos baseados em IA Generativa antes da disponibilização em produção. O processo pode abranger configuração do modelo, definição de instruções, associação de bases documentais, criação de mecanismos de proteção, execução de testes e avaliação da qualidade das respostas.
- O treinamento e o refinamento do comportamento do assistente consideram os requisitos específicos do projeto, os conteúdos autorizados pela CONTRATANTE e os resultados dos testes. Conforme a tecnologia adotada, esse processo pode envolver configuração de instruções, exemplos, intenções, entidades, recuperação de conhecimento e, quando aplicável, ajuste especializado do modelo.

- A capacidade de aprendizado ocorre por meio de um processo controlado de coleta, avaliação, curadoria e publicação de novos conhecimentos. As interações não alteram automaticamente o comportamento do ambiente produtivo sem validação, preservando a governança, a previsibilidade e a qualidade das respostas.
- O SmartBot Pro possui motor cognitivo capaz de processar linguagem natural, identificar intenções, extrair entidades, preservar contexto e conduzir jornadas automatizadas. O motor pode combinar fluxos estruturados, modelos de compreensão de linguagem, recuperação de conhecimento e IA Generativa.
- A base de conhecimento pode ser administrada em formato de perguntas e respostas, permitindo cadastrar, revisar, organizar e desativar conteúdos. Também podem ser associados sinônimos, categorias, documentos, períodos de validade e informações de contexto para melhorar a recuperação da resposta adequada.
- A construção das jornadas é realizada por editor visual de abordagem *low-code/no-code*. Usuários autorizados podem configurar mensagens, perguntas, condições, integrações, ações e transições sem necessidade de desenvolvimento em linguagem de programação estruturada.
- As entidades permitem identificar e extrair informações relevantes do texto, como nomes, documentos, datas, localidades, produtos, números de protocolo e demais termos específicos do negócio. Os valores extraídos podem ser utilizados em validações, decisões, consultas e integrações.
- Entidades semelhantes podem ser agrupadas em categorias e associadas a sinônimos, variações linguísticas e valores normalizados. Esse tratamento permite que diferentes formas de expressão sejam interpretadas como uma mesma informação de negócio.
- O editor de fluxos permite criar saltos condicionais, reutilizar blocos e subfluxos e coletar múltiplas informações por meio de slots. Os dados obtidos podem ser mantidos em variáveis de contexto e utilizados nas etapas seguintes da jornada.
- O contexto da conversa é preservado durante a sessão para evitar a repetição desnecessária de informações e possibilitar diálogos mais naturais. A memória conversacional observa o período de retenção, as regras de privacidade e os limites estabelecidos para cada jornada.
- O motor cognitivo classifica o assunto e a intenção do usuário a partir do conteúdo da mensagem, do contexto anterior e dos modelos configurados. Quando o nível de confiança não for suficiente, a solução pode solicitar esclarecimentos, apresentar alternativas ou encaminhar a interação para atendimento humano.
- A interação em Português do Brasil contempla perguntas e respostas formuladas em linguagem natural, incluindo variações usuais de vocabulário e construção de frases. O assistente pode fazer perguntas complementares para obter os dados necessários e selecionar a resposta ou ação mais adequada.
- Os diálogos podem ser diferenciados por perfil de usuário, canal, assunto, produto, unidade, horário ou contexto de atendimento. As condições de entrada permitem apresentar jornadas específicas para públicos distintos dentro do mesmo ambiente.
- Os recursos de NLG e IA Generativa permitem elaborar respostas com base nos documentos e conteúdos autorizados pela CONTRATANTE. A recuperação de conhecimento pode restringir a resposta às fontes disponibilizadas, reduzindo a geração de informações sem fundamentação e permitindo registrar as referências utilizadas.
- Durante a conversa, o usuário pode corrigir uma informação anteriormente fornecida. O assistente atualiza a variável correspondente e reavalia as condições subsequentes do fluxo, evitando que o dado incorreto continue sendo utilizado.
- O processamento de linguagem natural permite identificar, em uma única resposta, informações adicionais além daquelas solicitadas. Os dados reconhecidos podem preencher antecipadamente diferentes campos ou slots, reduzindo a quantidade de perguntas necessárias.
- A solução considera construções negativas na interpretação das mensagens, diferenciando afirmações, recusas, restrições e correções. Esse recurso contribui para que respostas como “não quero”, “não é esse” ou “ainda não recebi” sejam tratadas conforme o contexto.

- A manutenção do contexto permite interpretar referências a elementos mencionados anteriormente, incluindo pronomes, expressões resumidas e referências anafóricas. A precisão desse entendimento depende da clareza da conversa, da extensão do contexto preservado e da configuração do modelo utilizado.
- Subdiálogos podem ser acionados dentro da jornada principal para tratar assuntos complementares, validar informações ou executar consultas específicas. Após a conclusão do subfluxo, o atendimento pode retornar ao ponto correspondente do diálogo principal.
- Os fluxos podem combinar perguntas aninhadas, condições, saltos, variáveis, intenções e entidades para aprofundar o entendimento da solicitação. A lógica configurada permite adaptar o percurso da conversa às respostas fornecidas e entregar orientações mais precisas.
- As funcionalidades de Workforce Management utilizam técnicas estatísticas, séries temporais, modelos de filas e métodos de dimensionamento, incluindo Erlang C quando adequado à operação. Forecasting, Scheduling, Intraday Management e Adherence são funcionalidades de negócio e não possuem RFC específica.
- A governança dos recursos de Inteligência Artificial pode ser alinhada à ISO/IEC 42001, relacionada ao sistema de gestão de IA, à ISO/IEC 23894, voltada à gestão de riscos de IA, e à ISO/IEC 27001:2022, aplicada à segurança da informação. A avaliação da qualidade de sistemas de IA também pode considerar a ISO/IEC 25059.
- Quando as integrações utilizarem APIs Web, a troca de informações pode observar HTTP conforme a RFC 9110, JSON conforme a RFC 8259, OAuth 2.0 conforme a RFC 6749 e JWT conforme a RFC 7519. A proteção das comunicações pode utilizar TLS conforme as RFCs 8446 e 8996.
-
- Os fluxos existentes podem ser reutilizados como base para novos diálogos, mantendo blocos, intenções, entidades e regras já validadas. O conteúdo pode ser especializado ou enriquecido para diferentes domínios, produtos, canais e públicos, reduzindo o esforço de construção e facilitando a manutenção.
- A plataforma permite utilizar expressões regulares para identificar, extrair e validar padrões presentes nas mensagens dos usuários. As expressões podem ser combinadas com entidades, variáveis de contexto e respostas recebidas para validar documentos, números, códigos, datas e outros formatos definidos pelo projeto.
- As regras de diálogo podem combinar intenções, entidades, variáveis de contexto e operadores lógicos. Essas expressões permitem criar decisões com condições simples ou compostas, direcionando a conversa conforme as informações identificadas durante o atendimento.
- As entidades de sistema contemplam o tratamento de datas, horários, períodos e expressões temporais relativas. Termos como “hoje”, “amanhã”, “ontem”, “na próxima semana” ou “daqui a duas horas” podem ser convertidos em valores estruturados, considerando a data, o horário e o fuso da interação.
- Os recursos de análise conversacional permitem identificar perguntas com baixo nível de compreensão, intenções semelhantes, classificações conflitantes e mensagens não reconhecidas. Essas ocorrências podem ser revisadas pela equipe de curadoria para aprimoramento dos conteúdos e dos modelos cognitivos.
- O SmartBot Pro integra-se ao ambiente de telefonia da Plataforma Smartspace, utilizando serviços de transcrição e síntese de voz. O conteúdo falado pelo usuário é convertido em texto para processamento cognitivo, enquanto as respostas produzidas pelo assistente podem ser sintetizadas e reproduzidas durante a chamada.
- O ambiente de desenvolvimento permite testar e depurar os fluxos conversacionais antes da publicação. Nas integrações de voz, os usuários autorizados podem analisar etapas executadas, variáveis, intenções, transcrições e áudios associados aos testes, respeitando as políticas de acesso e proteção de dados.
- As APIs são documentadas em formato compatível com a especificação OpenAPI, disponibilizando a descrição dos recursos, parâmetros, métodos, estruturas de dados, códigos de retorno e mecanismos de autenticação. A documentação estruturada facilita testes, geração de clientes e integração com sistemas externos.

- O ciclo de evolução das APIs contempla controle de versões para reduzir impactos sobre as integrações existentes. Novas versões podem coexistir durante períodos de transição, com identificação explícita, documentação das alterações e política de descontinuação aplicável.
- As listas de contatos permitem configurar campos conforme as necessidades de cada campanha. Além dos campos predefinidos, usuários autorizados podem incluir, remover ou personalizar atributos utilizados para identificação, segmentação, roteamento e tratamento dos registros.
- A gestão de campanhas é realizada por interface administrativa, permitindo acompanhar listas, grupos, atendentes, resultados e indicadores operacionais. Conforme as permissões configuradas, os supervisores podem iniciar, pausar, retomar ou encerrar campanhas e sequências de campanhas.
- Os parâmetros das campanhas podem ser ajustados durante sua execução, incluindo taxa de rediscagem ou reenvio, intervalo entre tentativas, nível de ocupação, disponibilidade de agentes e modo de discagem. As alterações são aplicadas de maneira controlada, preservando os registros e as regras regulatórias da operação.
- O gerenciamento das listas permite consultar, incluir, alterar e excluir registros, além de associar diferentes meios de contato ao mesmo cliente, como telefone residencial, comercial e celular. Filtros e critérios de segmentação podem ser configurados para determinar quais registros serão utilizados em cada campanha.
- Os recursos de Speech Analytics permitem identificar os termos, expressões, assuntos e categorias mais recorrentes nas interações analisadas. Os resultados podem ser apresentados em listas, rankings, nuvens, árvores de palavras ou outros formatos gráficos disponíveis no ambiente analítico.
- A solução pode ser dimensionada para transcrever e analisar o conteúdo das chamadas de voz e das interações textuais abrangidas pelo escopo. As análises podem considerar palavras-chave, assuntos, categorias, sentimentos, silêncios, interrupções e demais indicadores habilitados, observadas a qualidade dos áudios, o idioma e as regras de privacidade.
- As avaliações podem gerar feedbacks estruturados para os agentes, contendo resultados, orientações, pontos de melhoria e informações do atendimento avaliado. As notificações e os relatórios ficam disponíveis no ambiente da plataforma conforme os perfis de acesso e o fluxo de ciência definido pela operação.
- Os dashboards apresentam informações históricas e em tempo real sobre atendimento, produtividade, filas, campanhas e experiência do cliente. Indicadores como CSAT e NPS podem ser obtidos por pesquisas configuradas na plataforma ou por integração mantida no escopo da solução, sem necessidade de ferramenta adicional para a CONTRATANTE quando assim previsto na proposta.
- As transcrições são armazenadas com controles que impedem alterações por usuários comuns e preservam sua vinculação ao atendimento original. A integridade pode ser reforçada por controle de acesso, trilhas de auditoria, versionamento, registros de data e hora e mecanismos de verificação do conteúdo.
- Os áudios gravados podem ser processados pelo serviço de Speech-to-Text, com armazenamento do texto associado à respectiva interação. Usuários autorizados podem pesquisar palavras, expressões, categorias, datas, agentes e demais atributos indexados.
- Os dados da plataforma são armazenados continuamente em serviços relacionais e/ou NoSQL, selecionados conforme a natureza das informações e os requisitos de desempenho. A arquitetura contempla escalabilidade, baixa latência, integridade, alta disponibilidade, rastreabilidade e auditoria, utilizando regiões de nuvem pública localizadas no território brasileiro para os dados abrangidos pelo contrato.
- O reconhecimento de linguagem natural em Português do Brasil pode utilizar modelos acústicos e linguísticos associados a dicionários, vocabulários e termos específicos do negócio. A interpretação pode ocorrer por correspondência semântica com comandos ou por classificação cognitiva da intenção expressa pelo usuário.
- Os componentes conversacionais podem ser reutilizados em URA vocal, chatbot, WhatsApp, Web Chat e demais canais suportados. As regras de negócio são compartilhadas sempre que aplicáveis, enquanto mensagens, tempos de resposta e formas de interação podem ser adaptados às características de cada canal.
- Os Assistentes Virtuais podem operar nos canais digitais e de voz suportados e contratados, utilizando IA Generativa, processamento de linguagem natural e gerenciamento de contexto. As interações são registradas

e podem ser concluídas automaticamente ou transferidas para atendimento humano com preservação do histórico e das informações coletadas.

- O editor visual permite construir árvores de decisão com perguntas, respostas, condições, integrações, mensagens e regras de direcionamento. Perguntas de esclarecimento podem ser utilizadas quando a solicitação estiver incompleta, ambígua ou apresentar nível de confiança insuficiente.
- Como referência técnica, a integração com telefonia utiliza SIP conforme a RFC 3261, RTP e RTCP conforme a RFC 3550 e mídia segura por SRTP conforme a RFC 3711. A transmissão de eventos DTMF pode observar a RFC 4733, conforme o cenário de integração.
- As APIs Web podem utilizar HTTP conforme a RFC 9110, URIs conforme a RFC 3986 e estruturas JSON conforme a RFC 8259. Os controles de autenticação podem utilizar OAuth 2.0 conforme a RFC 6749 e tokens JWT conforme a RFC 7519, com proteção TLS conforme as RFCs 8446 e 8996.
- A documentação das integrações observa a OpenAPI Specification, preferencialmente em versão 3.x. O versionamento pode ser aplicado por URI, cabeçalho ou outro mecanismo documentado, acompanhado de política de compatibilidade e transição entre versões.
- Para recursos de voz, podem ser utilizadas especificações do W3C como Speech Synthesis Markup Language — SSML, Speech Recognition Grammar Specification — SRGS e VoiceXML, quando aplicáveis aos componentes adotados. Essas especificações não são RFCs, mas padrões técnicos voltados à interoperabilidade de aplicações de voz.
- A preservação das transcrições e demais evidências pode ser alinhada aos controles da ISO/IEC 27001:2022 e da ISO/IEC 27701, além dos requisitos da Lei Geral de Proteção de Dados. Quando utilizado carimbo de tempo eletrônico, sua implementação pode observar a RFC 3161.
- A árvore de decisão e os conteúdos do Assistente Virtual podem ser administrados diretamente por usuários autorizados da CONTRATANTE. A interface permite revisar perguntas não respondidas, corrigir classificações, associar mensagens a intenções existentes e publicar melhorias sem necessidade de intervenção recorrente da CONTRATADA.
- As mensagens recebidas são analisadas quanto ao conteúdo, à intenção, às entidades e ao contexto da conversa. A partir dessa interpretação, a plataforma seleciona o fluxo, a resposta, a integração ou o grupo de atendimento mais adequado para continuidade da jornada.
- A identidade do Assistente Virtual pode ser personalizada por meio de nome, linguagem, tom de comunicação, persona e avatar. Conforme os recursos permitidos pelo canal, as mensagens podem conter botões, links, imagens, emojis, listas e demais elementos interativos.
- As regras de negócio são centralizadas em ambiente gráfico e controladas por perfis de acesso. As áreas de negócio podem administrar conteúdos, fluxos e parâmetros autorizados, enquanto a área de TI mantém a governança das integrações, segurança, ambientes e componentes de maior criticidade.
- O processo de pesquisa pode ser configurado quanto ao público, canal, momento de aplicação, periodicidade, critérios de seleção, perguntas, escalas de resposta e regras de encerramento. Também podem ser estabelecidos limites para evitar pesquisas repetitivas ao mesmo usuário.
- A plataforma permite criar formulários de avaliação para interações de voz, texto e vídeo. Os modelos podem conter critérios objetivos, campos descritivos, notas, pesos, respostas obrigatórias, itens críticos e parâmetros de cálculo definidos pela operação.
- Os formulários suportam lógica condicional, permitindo apresentar ou ocultar campos conforme as respostas anteriores. Dessa forma, cada avaliação pode seguir um percurso específico, evitando perguntas desnecessárias e aprofundando a análise quando determinada condição for identificada.
- As pesquisas podem ser habilitadas ou desabilitadas por produto, serviço, operação, campanha, fila ou canal. A parametrização permite definir onde e quando o mecanismo será aplicado sem afetar as demais jornadas configuradas.
- O motor cognitivo correlaciona as perguntas atuais com as informações fornecidas anteriormente, preservando o contexto necessário para compreender a solicitação. As respostas são recuperadas ou elaboradas a partir dos conteúdos autorizados e das regras definidas para o atendimento.

- A plataforma combina NLU, NLP, Machine Learning e IA Generativa para identificar intenções e extrair entidades das mensagens. Informações como nomes, documentos, produtos, localidades, datas e protocolos podem ser convertidas em dados estruturados para utilização no fluxo.
- A memória conversacional permite considerar mensagens anteriores na seleção das respostas, evitando repetições e mantendo a coerência da jornada. O contexto é preservado dentro dos limites de sessão, retenção e privacidade estabelecidos para o projeto.
- A evolução do entendimento ocorre por processo controlado de análise, curadoria, testes e publicação. Perguntas não reconhecidas, novas expressões, conteúdos recorrentes e avaliações negativas podem ser utilizados para melhorar intenções, vocabulários, respostas e fontes de conhecimento, sem alteração automática e não supervisionada do ambiente produtivo.
- Os usuários podem formular perguntas livremente em Português do Brasil, sem necessidade de seguir comandos rígidos ou estruturas predefinidas. Quando necessário, o assistente pode solicitar informações complementares para esclarecer a intenção.
- Os modelos linguísticos podem tratar variações coloquiais, gírias, regionalismos, neologismos, abreviações e erros ortográficos comuns. A assertividade pode ser ampliada por meio da inclusão de exemplos, sinônimos e expressões próprias do contexto regional e institucional da CONTRATANTE.
- O vocabulário pode ser parametrizado com conceitos, entidades, siglas, produtos, localidades e termos específicos do negócio. Essa customização permite aproximar a linguagem do assistente daquela utilizada pelos cidadãos, atendentes e áreas responsáveis pelo serviço.
- As chamadas destinadas a números 0800, tridígitos e demais numerações configuradas podem ser recebidas diretamente pela infraestrutura central da plataforma. Nesse ambiente são executados o tratamento da URA, a gravação, o enfileiramento e o roteamento, sendo encaminhadas às posições de atendimento somente as chamadas atribuídas aos respectivos agentes.
- A centralização do tratamento evita a entrega indiscriminada das chamadas aos ambientes locais e permite aplicar políticas uniformes de segurança, gravação, distribuição e contingência. O encaminhamento às posições de atendimento considera disponibilidade, habilidade, prioridade, unidade e demais regras definidas pela CONTRATANTE.
- Os relatórios da URA apresentam a quantidade total de chamadas recebidas no período selecionado. Os dados podem ser filtrados por número de acesso, serviço, fluxo, unidade, faixa de horário e demais atributos disponíveis.
- As chamadas resolvidas ou encerradas no atendimento automatizado podem ser contabilizadas separadamente, permitindo medir a capacidade de retenção e conclusão da URA sem intervenção humana.
- As transferências para atendimento humano são registradas e apresentadas em valores absolutos e percentuais. Os indicadores podem ser detalhados por opção escolhida, fila de destino, serviço, horário e resultado da transferência.
- As perdas e os abandonos ocorridos durante a navegação na URA podem ser classificados por etapa e motivo, incluindo desligamento pelo usuário, ausência de resposta, tempo excedido, opção inválida ou falha técnica identificada.
- As perdas ocorridas durante a transferência para o atendimento humano podem ser diferenciadas por motivo, como abandono em fila, indisponibilidade de agentes, tempo de espera excedido, falha de roteamento ou desconexão durante a tentativa de entrega.
- As escolhas efetuadas pelos usuários nos menus da URA são consolidadas em valores absolutos e percentuais. Essas informações permitem identificar as opções mais utilizadas, pontos de abandono e oportunidades de simplificação da jornada.
- Os relatórios estatísticos permitem identificar a Hora de Maior Movimento e o Dia de Maior Movimento, considerando o período analisado. Os indicadores podem apoiar o dimensionamento de canais, agentes, filas e recursos de infraestrutura.

- Como referência técnica, o tratamento das chamadas utiliza SIP conforme a RFC 3261 e RTP/RTCP conforme a RFC 3550. Os eventos DTMF podem ser transmitidos conforme a RFC 4733, enquanto informações de identidade, motivo e histórico de redirecionamento podem observar as RFCs 3325, 3326, 5806 e 7044.
- A proteção da sinalização pode utilizar SIP sobre TLS e SIPS conforme as RFCs 3261 e 5630, enquanto a proteção da mídia pode utilizar SRTP conforme a RFC 3711. A marcação de qualidade de serviço pode observar as RFCs 2474 e 4594.
- Os elementos interativos dos canais digitais seguem as capacidades técnicas de cada canal. Links utilizam a estrutura de URI definida pela RFC 3986; conteúdos Web podem utilizar HTTP conforme a RFC 9110; e a representação de emojis e caracteres observa o padrão Unicode aplicável.
- Os recursos de Inteligência Artificial podem ser governados por controles alinhados à ISO/IEC 42001, ISO/IEC 23894 e ISO/IEC 27001:2022. As práticas de atendimento e avaliação da experiência do cliente também podem considerar a ISO 18295-1, aplicável a centros de contato com clientes.
-
- A plataforma controla a associação de cada mensagem SMS ao respectivo fluxo e contexto de atendimento. Quando uma nova mensagem inicia uma jornada diferente, o fluxo anterior pode ser encerrado automaticamente, mantendo apenas uma sessão ativa por usuário, conforme as regras de correlação e expiração configuradas.
- Os fluxos conversacionais podem ser validados em ambiente de laboratório ou homologação antes da publicação. O ambiente permite simular entradas, percorrer árvores de decisão, verificar variáveis, intenções, integrações e respostas sem disponibilizar a versão em teste aos usuários finais.
- A solução contempla discador automático integrado ao Contact Center, permitindo configurar campanhas, listas, agentes, horários, tentativas, resultados e regras de contato. A execução e o acompanhamento das discagens são realizados pela própria plataforma.
- Na discagem sob demanda ou *Preview Dialer*, os dados disponíveis do cliente são apresentados ao agente antes da chamada. O agente pode analisar as informações e decidir pelo início da discagem sem digitar manualmente o número telefônico.
- Na discagem progressiva, uma nova tentativa é iniciada automaticamente quando um agente compatível fica disponível. Essa modalidade busca reduzir a ociosidade sem realizar chamadas antecipadas sem a correspondente capacidade de atendimento.
- O modo *Power Dialer* permite definir uma taxa de sobrediscagem para estabelecer uma ou mais tentativas conforme a disponibilidade dos agentes. O parâmetro pode ser ajustado de acordo com a taxa de completamento, a ocupação desejada e as regras da campanha.
- Na discagem preditiva, algoritmos estatísticos analisam o comportamento da campanha para estimar o momento e a quantidade apropriada de tentativas. O objetivo é aumentar a produtividade, mantendo controle sobre o nível de abandono e a disponibilidade efetiva dos agentes.
- O algoritmo preditivo pode considerar Tempo Médio de Atendimento, Tempo Médio de Operação, Tempo Médio de Espera, quantidade de agentes disponíveis ou em chamada, taxa de completamento, duração das tentativas e resultados históricos.
- Todas as tentativas são registradas, incluindo chamadas atendidas, não atendidas, ocupadas, inválidas, sem resposta, reagendadas ou encerradas por outros motivos. Os registros permitem acompanhar a efetividade da campanha e o histórico de contato de cada cliente.
- Quando ocorrer abandono antes do atendimento, a plataforma pode registrar uma solicitação de retorno e iniciar automaticamente uma nova chamada. Após a confirmação do cliente, o contato é encaminhado para um agente previamente reservado ou selecionado conforme as regras de habilidade, prioridade e disponibilidade.
- As políticas de retorno podem priorizar o mesmo atendente responsável pela interação anterior. Quando ele não estiver disponível dentro do período definido, a chamada pode ser encaminhada para outro agente habilitado, evitando espera excessiva.

- A integração com o WhatsApp utiliza números vinculados à WhatsApp Business Platform e devidamente aprovados no processo de ativação da Meta. A CONTRATANTE pode indicar números de sua faixa de numeração, inclusive números fixos elegíveis, desde que atendidos os requisitos de titularidade, verificação e uso estabelecidos para o canal.
- O Assistente Virtual pode responder e concluir jornadas diretamente no canal utilizado pelo cliente. A intervenção humana ocorre somente quando prevista pelo fluxo, solicitada pelo usuário ou necessária em razão de uma exceção, baixa confiança ou regra de negócio.
- O atendimento em redes sociais pode ser integrado à interface omnichannel por meio de conectores e APIs oficiais disponíveis para Facebook, Instagram, X e LinkedIn. A cobertura de mensagens, comentários e publicações depende das permissões, modalidades de conta e recursos disponibilizados por cada rede social.
- Os adaptadores monitoram as atividades às quais a CONTRATANTE possua acesso autorizado, transformando mensagens, comentários, menções ou outros eventos suportados em interações tratáveis. Alterações ou restrições das APIs oficiais podem exigir adequação dos conectores.
- Regras de monitoramento podem identificar palavras, frases, combinações de termos e padrões definidos pela CONTRATANTE. As ocorrências podem gerar demandas internas, classificações, alertas ou encaminhamentos para equipes responsáveis.
- A análise de sentimento classifica o conteúdo como positivo, neutro ou negativo e pode ser utilizada em conjunto com assunto, prioridade e canal. A classificação automática serve como apoio à triagem e pode ser revisada quando o contexto apresentar ambiguidade, ironia ou linguagem figurada.
- Temas sociais ou institucionais de maior interesse podem ser monitorados por vocabulários, categorias e regras parametrizadas. Os resultados podem ser priorizados conforme recorrência, alcance, criticidade ou outros indicadores disponibilizados pelo canal integrado.
- A plataforma permite enviar e receber anexos por e-mail e pelos canais digitais compatíveis, incluindo WhatsApp, Telegram, Messenger, Instagram Direct e outros serviços habilitados. Tipos, tamanhos e formas de envio permanecem sujeitos às limitações de cada API oficial.
- Os arquivos podem ser mantidos temporariamente na infraestrutura da solução durante o intercâmbio entre clientes e atendentes. O armazenamento contempla controle de acesso, prazo de retenção e descarte após o período configurado, evitando a gravação direta no ambiente tecnológico da CONTRATANTE.
- A solução trata arquivos nos formatos PDF, JPG, JPEG, PNG, DOC, DOCX, TXT, GIF, CSV, XLS, XLSX, MP3, MP4, ZIP e RAR, observadas as restrições do canal, tamanho máximo, políticas de segurança e capacidade de visualização. TIFF, GDOC e GSHEET podem ser tratados quando disponibilizados em formato compatível ou mediante integração aplicável.
- Mensagens de áudio recebidas por WhatsApp e Telegram podem ser reproduzidas diretamente na interface do agente. O arquivo permanece associado ao histórico da interação e pode ser submetido à transcrição quando esse recurso estiver habilitado.
- Os agentes possuem acesso a uma biblioteca de respostas rápidas, textos padronizados e conteúdos recorrentes. As mensagens podem ser organizadas por categoria, fila, assunto ou canal, respeitando as permissões e regras de uso.
- Novas solicitações podem gerar alertas visuais, sonoros ou destaques na interface de atendimento. O comportamento das notificações pode considerar a fila, prioridade, tempo de espera e estado operacional do agente.
- Mensagens automáticas podem ser configuradas por fila para informar recebimento, posição, indisponibilidade, prazo estimado, horário de atendimento ou outras orientações. O disparo pode ocorrer com base em regras, eventos e categorizações, sem intervenção manual do atendente.
- Cada agente pode conduzir pelo menos cinco sessões simultâneas de chat, sendo o limite parametrizável conforme o canal, o perfil do usuário e a complexidade da operação. O controle de simultaneidade evita a atribuição de novas interações quando o limite configurado for atingido.

- A plataforma permite configurar mensagens informativas automáticas ou enviadas manualmente pelo agente. O conteúdo pode variar conforme canal, fila, etapa da jornada, horário ou evento identificado durante o atendimento.
- A partir de uma interação corrente, o agente pode iniciar uma comunicação por outro meio, como migrar de chat para voz ou vídeo, desde que o canal esteja habilitado e existam os dados e consentimentos necessários. O histórico permanece relacionado ao mesmo atendimento ou protocolo.
- A transferência para o segundo nível preserva o conteúdo da conversa, os dados coletados, anexos, classificações e demais informações disponíveis. O novo atendente recebe o contexto da interação, enquanto o cliente pode ser informado automaticamente sobre o encaminhamento.
- Informações confidenciais podem ser coletadas por mecanismos protegidos e ocultadas da visualização do atendente. Os campos sensíveis podem utilizar mascaramento, restrição de acesso, criptografia ou formulários seguros, conforme o canal e a política definida pela CONTRATANTE.
- A comunicação pode combinar texto, áudio, vídeo, imagens e arquivos dentro dos recursos suportados pelos canais habilitados. A mudança de modalidade durante a conversa preserva o contexto e a identificação da interação sempre que tecnicamente suportada.
- A personalização do Assistente Virtual contempla identificação de intenções, extração de entidades, configuração do vocabulário e construção das regras de condução. O processamento ocorre em tempo compatível com a conversação, permitindo resolver, esclarecer ou encaminhar a necessidade apresentada pelo usuário.
- A implantação inclui a configuração da identidade visual, carga dos conteúdos fornecidos pela CONTRATANTE, estruturação das intenções e construção dos fluxos de atendimento. A publicação é precedida por validação funcional e homologação das jornadas definidas.
- Como referência técnica, as integrações de voz utilizam SIP conforme a RFC 3261 e RTP/RTCP conforme a RFC 3550. Funcionalidades multimídia e WebRTC podem observar as RFCs 8825, 8866, 8445, 5764 e 3711.
- As comunicações de chat em tempo real podem utilizar WebSocket conforme a RFC 6455, enquanto APIs e eventos utilizam HTTP conforme a RFC 9110 e JSON conforme a RFC 8259. A autenticação pode utilizar OAuth 2.0 e JWT conforme as RFCs 6749 e 7519.
- O envio de e-mails e anexos pode observar SMTP conforme a RFC 5321, o formato de mensagens conforme a RFC 5322 e as extensões MIME conforme as RFCs 2045 a 2049. A classificação dos tipos de mídia pode seguir a RFC 6838.
- A proteção do transporte utiliza TLS conforme as RFCs 8446 e 8996. Os controles de armazenamento, acesso, retenção e proteção de informações pessoais podem ser alinhados à ISO/IEC 27001:2022, ISO/IEC 27701 e à LGPD.
- Os recursos de IA podem ser governados segundo a ISO/IEC 42001 e a ISO/IEC 23894, contemplando gestão de riscos, supervisão humana, curadoria, rastreabilidade e controle da evolução dos modelos.

4.1.2 Sobrevivência local

O módulo de sobrevivência local da Plataforma SMARTSPACE é projetado para soluções de grande porte com estrutura centralizada de autenticação e roteamento, garantindo a continuidade das operações em localidades remotas mesmo em cenários de falhas ou perda de conectividade com o core central.

- **Gestão centralizada:** A administração dos equipamentos de sobrevivência local é realizada de forma centralizada pela Plataforma SMARTSPACE, garantindo simplicidade e eficiência no gerenciamento.

- **Operação transparente:** O módulo de sobrevivência local, instalado em um servidor ou gateway dedicado, entra em operação automaticamente e de forma transparente em caso de indisponibilidade do core central ou perda de conectividade.
- **Funcionalidades completas em modo de sobrevivência:** Durante a ativação, o sistema mantém todas as características e funcionalidades originais do core central, incluindo:
    - Discagem por senha.
    - Controle e roteamento de chamadas.
    - Criptografia de sinalização e mídia (DTLS/TLS e SRTP).
    - Música em espera, anúncios e tons.
    - Integrações com sistemas.
    - Geração de bilhetes CDR.
    - Recursos como hot desking (free seating).
    - Conectividade com a PSTN local.
- **Servidor de mídia local:** O módulo também funciona como servidor de mídia local, oferecendo serviços como músicas de espera, tons e áudios de URA, sem a necessidade de tráfego de voz até o core central da solução.
- **Integração com principais fabricantes:** A sobrevivência local possui integração nativa com gateways homologados, como Khomp e AudioCodes, além de servidores dedicados ou virtualizados. Isso preserva as funcionalidades completas da solução, garantindo que localidades remotas mantenham recursos avançados mesmo em modo de sobrevivência.
- **Capacidade escalável:** Nos gateways homologados, como os da AudioCodes e Khomp, o módulo de sobrevivência suporta até 50.000 usuários por equipamento, dependendo do modelo. Para localidades com maior quantidade de usuários, é possível adicionar servidores dedicados para garantir a capacidade necessária.
- **Recursos avançados durante a sobrevivência:**
    - **Media server local:** Música em espera, tons e anúncios, além de transcoding entre os gateways e a rede interna, maximizando a eficiência dos equipamentos, independentemente do codec utilizado.
    - **Funcionalidades locais:** URA, filas de atendimento, gravação de chamadas e demais módulos permanecem ativos.
    - **Sincronização automática:** Todas as informações processadas durante o período de sobrevivência são armazenadas localmente e sincronizadas com o core central assim que a comunicação é restabelecida. Essa sincronização ocorre de forma transparente para os usuários e pode ser monitorada pela interface web.
- **Cobertura total dos módulos:** Todos os módulos da Plataforma SMARTSPACE (PABX IP, URA, Contact Center, Gravador, entre outros) possuem suporte total ao módulo de sobrevivência local.

5 Criptografia e Segurança

A Plataforma Smartspace oferece suporte nativo aos principais protocolos de criptografia e segurança amplamente adotados no mercado, assegurando que todas as comunicações, sejam entre os módulos ou entre usuários, ocorram exclusivamente por meio de canais criptografados. Essa abordagem garante integridade, confidencialidade e proteção contra interceptações ou acessos não autorizados.

A Plataforma SMARTSPACE adota mecanismos robustos de segurança cibernética baseados em criptografia de ponta a ponta e controle de admissão na borda. Toda a sinalização SIP é blindada por meio do protocolo TLS (versões 1.2 e 1.3), enquanto o tráfego de mídia é integralmente criptografado via SRTP com algoritmos AES-256 e DTLS, o que impede qualquer tipo de interceptação ou escuta não autorizada. Complementarmente, o ecossistema valida o perímetro de segurança utilizando autenticação SIP Digest (padrão cliente/servidor) e suporte a barramentos de identidade corporativa via RADIUS Digest e HTTPS para gerência, além de exigir Autenticação Multifator (MFA) para perfis administrativos e permitir a restrição e o bloqueio automático de registros por faixas de endereços IP autorizados, garantindo total rastreabilidade, auditoria e estrita conformidade com a LGPD.

5.1 Especificações Técnicas

- **Acesso seguro:** Interface de gerência e monitoramento protegida por conexão HTTPS, garantindo a confidencialidade dos dados transmitidos.
- **Controle de acesso:** Usuários autenticados por credenciais (usuário e senha) com perfis configuráveis e níveis de permissão customizáveis, adequados às necessidades do ambiente.
- **Segurança contra inatividade:** Desconexão automática de usuários logados nas interfaces de gerência após períodos de inatividade, reforçando a proteção contra acessos não autorizados.
- **Criptografia de mídia:** Suporte ao transporte de mídia RTP e SRTP com encriptação através de algoritmos AES-128 e AES-256, utilizando chaves simétricas, dinâmicas e únicas para cada sessão.

- **Abrangência de criptografia:** Proteção de chamadas de áudio, vídeo, conteúdo compartilhado e chats em todos os tipos de endpoints, com senhas de dispositivos protegidas e personalizadas.
- **Flexibilidade de configuração:** Criptografia configurável como mandatória, opcional ou desabilitada, conforme as demandas específicas do projeto.
- **Troca dinâmica de chaves:** Realizada a cada chamada por meio de canais criptografados, garantindo segurança adicional.
- **Criptografia de sinalização:** Suporte nativo aos protocolos DTLS e TLS (versões 1.0, 1.1, 1.2 e 1.3) para proteger a sinalização SIP.
- **Integração com dispositivos:** Permite uso de protocolo TLS entre dispositivos IP da plataforma e o controlador de chamadas, assegurando comunicações seguras.
- **Bloqueio de dispositivos inseguros:** Possibilidade de configurar bloqueio de dispositivos que não utilizem TLS, evitando vulnerabilidades.
- **Criptografia em dispositivos analógicos:** A proteção acontece até o último endpoint IP, garantindo segurança mesmo quando dispositivos analógicos, como ATA, estão conectados via TDM.
- **Compatibilidade com IPSec:** Suporte nativo ao protocolo IPSec, oferecendo camadas adicionais de segurança para comunicação de rede.
- **Certificados digitais:**
    - Geração de certificados autoassinados ou assinados por CA externas.
    - Suporte a certificados X.509 (todas as versões), assinados ou não por autoridades certificadoras externas.
    - Compatibilidade com o modelo de chaves PKI (Public Key Infrastructure).
    - Certificados com SHA256-RSA-4096Bits, SHA256-RSA-2048Bits, entre outros padrões avançados de criptografia.
- **Proteção de comunicação SIP:**
    - Suporte a criptografia para comunicação com qualquer endpoint SIP e em entroncamentos SIP.
    - Transferência de chamadas criptografada entre servidores IP PBX de diferentes localidades.
    - Criptografia nativa na comunicação com Gateways de voz via SIP.
- **Restrição de dispositivos e aplicações:**
    - Possibilidade de bloquear portas USB e restringir a instalação de aplicações não registradas ou não homologadas pela plataforma.
- **Antivírus integrado:** Suporte para proteção contra ameaças, como trojans, worms, vírus e outras vulnerabilidades.

- **Segurança proativa:**
    - Bloqueio automático após múltiplas tentativas de registros SIP ou logins no sistema com falhas, prevenindo ataques de força bruta.
    - Monitoramento detalhado com logs e informações específicas relacionadas à segurança do sistema.
- **Armazenamento seguro de logs:**
    - Suporte a armazenamento externo de logs de auditoria, com recursos de proteção e monitoramento de segurança para procedimentos de acesso.
    - Logs de auditoria são salvos em banco de dados e em arquivos criptografados, centralizando as informações com mecanismos de segurança aplicados.
    - Os logs podem ser exportados diretamente a partir da ferramenta de gerenciamento web do sistema Smartspace.
- **Firewall e proteção avançada:**
    - Firewall interno com suporte a bloqueio automático após um número configurável de tentativas inválidas de login, seja de usuários locais ou LDAP.
    - Proteção contra ataques DoS/DDoS, incluindo SYN floods, ping floods, finger of death, e outros tipos de ameaças.
    - Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) integrados.
    - A solução conta com um laboratório de segurança de classe mundial, dedicado ao aprimoramento contínuo das tecnologias de defesa contra ataques cibernéticos. Este laboratório trabalha em conjunto com uma rede de parceiros globais especializados, garantindo que os sistemas estejam sempre atualizados e preparados para prevenir novos tipos de ameaças e ataques emergentes.
- **Auditoria detalhada e centralizada:**
    - Registros abrangentes que incluem acessos, sessões, comandos, atividades e modificações, criando trilhas completas para auditoria futura.
    - Logs específicos para atividades no sistema de gravação, como consultas, downloads e audições realizadas pelos usuários.
    - Todas as operações realizadas na plataforma (via WEB, CLI ou SOAP) são registradas em trilhas de auditoria, incluindo modificações em qualquer componente da solução.
    - Suporte para consultas diferenciadas nas trilhas de auditoria, com parâmetros e visões personalizáveis.
- **Proteção contra falhas e segurança de dados:**
    - Mecanismos que evitam que falhas em processos impactem o funcionamento da solução.

- Todos os dados confidenciais, como credenciais de acesso, dados históricos e configurações, são armazenados de forma criptografada. Não há arquivos de configuração em texto puro.

- **Monitoramento contínuo:**
  - Logs dedicados para auditoria de acessos ao CDR, informações do DAC, gravações, entre outros dados sensíveis.
  - Registro de tentativas de acesso indevidas e análise de eventos relacionados à segurança.

6 Licenciamento

A Plataforma SMARTSPACE apresenta um sistema de licenciamento altamente flexível, capaz de se adaptar a diferentes cenários e necessidades. A solução pode ser implementada em nuvem privada ou pública, assim como na estrutura do cliente, em ambientes on-premise.

- **Ativação de licenças:** Realizada por meio de arquivo de licença ou código de ativação on-line.
- **Controle distribuído ou centralizado:** Configurável de acordo com as necessidades do cliente dentro da Plataforma.
- **Independência de dispositivos físicos ou serviços externos:** Não exige nenhum dispositivo ou serviço externo para ativação ou controle do licenciamento.
- **Licenciamento flutuante:** Oferece a possibilidade de compartilhar licenças entre múltiplos sites ou definir uma quantidade específica para cada localidade.
- **Licenciamento por usuário:** Flexível, sem restrições nos recursos disponíveis para cada usuário.
- **Operação offline:** Não requer conexão com a Internet para controle das licenças.
- **Autonomia do sistema:** Todo o controle de licenciamento é integrado e gerido internamente pela Plataforma SMARTSPACE, sem dependência de serviços externos. Assim, o funcionamento da solução permanece inalterado, mesmo em casos de indisponibilidade, isolamento ou falhas de conectividade.
- **Isolamento de sites remotos:** Em casos de desconexão entre um site remoto e o Datacenter principal, a plataforma utiliza mecanismos locais para controle de licenças, garantindo operação contínua mesmo em longos períodos de isolamento.
- **Monitoramento e alertas:** Integrado ao SMARTSPACE MANAGER/MONIT, permitindo que os administradores acompanhem o status das licenças e recebam notificações sobre falhas ou uso excessivo.

- A solução de colaboração permite estabelecer conversas com áudio, vídeo, mensagens, compartilhamento de tela e troca de arquivos. Os recursos permanecem disponíveis para usuários cadastrados e convidados, conforme as permissões definidas para a sessão.
- As conferências comportam pelo menos 100 participantes e podem ser iniciadas diretamente pelo organizador. As salas podem operar com ou sem moderação, incluindo controle de entrada, convites e início programado ou manual.
- Participantes externos podem ingressar por link ou por chamada telefônica destinada à numeração associada à conferência. O acesso como convidado utiliza identificação e controles compatíveis com a política definida para a reunião.
- Reuniões programadas e encontros imediatos podem ser acessados pela Internet em computadores e dispositivos móveis. A sessão pode ser retomada em outro dispositivo preservando a sala, os participantes e o contexto da colaboração.
- A experiência Web é compatível com versões atuais de navegadores amplamente utilizados. Aplicativos móveis podem ser disponibilizados para iOS e Android, com acesso às funcionalidades autorizadas para cada dispositivo.
- Usuários podem localizar outros integrantes da organização, iniciar conversas e formar grupos sem depender exclusivamente da agenda local do equipamento. Mensagens individuais ou coletivas permanecem associadas ao ambiente corporativo.

- A capacidade é dimensionada para suportar simultaneidade equivalente a, no mínimo, 30% da base habilitada, com possibilidade de ampliação modular. O acompanhamento de consumo permite adequar os recursos aos períodos de maior utilização.
- A mídia utiliza adaptação às condições disponíveis de rede. Perfis de áudio podem operar a partir de aproximadamente 64 Kbps, enquanto vídeo utiliza referência inicial de 512 Kbps por fluxo, variando conforme resolução, codec, número de participantes e condições do acesso.
- A solução utiliza codecs padronizados para áudio e vídeo e reconhece câmeras USB ou integradas aos computadores e dispositivos móveis. O processamento de vídeo pode utilizar H.264, H.265, VP8, AV1 ou tecnologias compatíveis, conforme o cliente e o cenário de interoperabilidade.
- As sessões de colaboração podem ser gravadas com áudio, vídeo e compartilhamento de tela. A gravação pode ocorrer automaticamente para reuniões previamente configuradas ou ser controlada pelo responsável durante a sessão.
- Os participantes são informados sobre o início da gravação pelos recursos disponíveis na interface. O arquivo resultante preserva a experiência audiovisual da sessão dentro dos parâmetros de qualidade definidos para a transmissão.
- As gravações ficam reunidas em repositório Web com acesso controlado. Usuários autorizados podem pesquisar, reproduzir e baixar conteúdos utilizando atributos como data, participante e identificação da reunião.
- Os arquivos podem ser disponibilizados em formatos amplamente reconhecidos, incluindo MP4 para vídeo e MP3 para áudio. Exportações em lote e integrações com repositórios externos podem ser realizadas por mecanismos controlados e APIs documentadas.
- Os conteúdos armazenados utilizam proteção criptográfica durante a transmissão e em repouso. Ações de consulta, reprodução, download, exportação e administração podem ser registradas para fins de rastreabilidade.
- O serviço de voz é baseado em arquitetura SIP e pode atender terminais IP Wi-Fi, dispositivos DECT IP, softphones e identidades virtuais. A associação do usuário ao recurso de voz pode ser ajustada sem perder suas permissões e facilidades.
- A infraestrutura funciona em nuvem com isolamento lógico entre ambientes. Os serviços de comunicação podem ser compostos por módulos especializados, apresentados aos usuários e administradores como uma solução integrada.
- Entroncamentos SIP permitem conexão com operadoras, gateways, centrais de atendimento e servidores de voz de diferentes fabricantes. A sinalização segue a RFC 3261 e pode operar com tráfego de entrada, saída ou bidirecional.
- Os troncos admitem expansão modular e podem ser configurados com faixas de numeração próprias. O plano de discagem trata códigos de país, DDD, números locais, formatos E.164 e normalização entre os diferentes padrões utilizados nas integrações.
- A mídia de voz contempla G.711 A-law, G.711 µ-law, G.729 e Opus, conforme negociação entre os elementos participantes. A priorização do tráfego pode utilizar marcações ToS e DSCP.
- A conectividade considera redes com NAT e firewall, incluindo mecanismos de STUN, TURN e ICE quando aplicáveis. A qualidade final depende também da largura de banda, latência, perda, variação de atraso e políticas implementadas na rede corporativa.
- A sinalização pode ser protegida por TLS 1.2 ou superior e a mídia por SRTP. O SBC aplica controle de sessões, ocultamento da topologia, normalização SIP, inspeção stateful, limitação de tráfego e proteção contra comportamentos anômalos.
- A Plataforma Smartspace pode operar com Session Border Controller (SBC) como elemento de proteção e interconexão das sessões de voz sobre IP. O SBC realiza o controle e a normalização do tráfego de sinalização e mídia, apoiando a interoperabilidade entre ramais, plataformas de comunicação e troncos SIP. Sua utilização pode ser dimensionada conforme a capacidade, a topologia e as políticas de segurança de cada ambiente.
- Na borda SIP, o SBC aplica controle de acesso, validação de sessões, inspeção de mensagens e cabeçalhos, limitação de tráfego e bloqueio de origens não autorizadas. As regras de firewall SIP podem ser configuradas por endereço, domínio, usuário, tronco e interconexão. A identificação de comportamentos anômalos e o controle de admissão contribuem para a proteção contra registros indevidos, mensagens SIP malformadas e ataques de negação de serviço.
- O SBC controla a negociação de mídia nas interconexões SIP, considerando os codecs habilitados, a ordem de preferência configurada e a compatibilidade entre os elementos envolvidos na chamada. A arquitetura de

voz da Plataforma Smartspace contempla codecs como G.711 A-law e µ-law, G.722, G.729, G.729A, G.729AB e Opus, entre outros disponíveis conforme os componentes e perfis de integração utilizados.

- processamento seguro de fluxos de voz estruturados nos codecs Opus-NB/WB, SILK-NB/WB
- , AMR-WB (G.722.2), AMR-NB, G.711 (A-law/u-law) e G.729A/B
- O tratamento de áudio da solução inclui mecanismos de detecção de atividade de voz, supressão de silêncio, geração de ruído de conforto e compensação dinâmica de jitter. Esses recursos contribuem para a continuidade e a inteligibilidade da comunicação em redes sujeitas a variações de atraso e perda de pacotes.
- Na borda de comunicação, o SBC controla as sessões e aplica as políticas de interconexão aos fluxos de sinalização e mídia. A solução admite SIP sobre TLS e proteção da mídia por SRTP, com parâmetros definidos de acordo com os elementos integrados e a política de segurança do ambiente. O SBC também executa inspeção, normalização e controle do tráfego SIP, inclusive em cenários com tradução de endereços.
- As políticas de interconexão do SBC permitem definir rotas para o encaminhamento das sessões SIP e estabelecer regras distintas por tronco, domínio, origem e destino. A integração com a infraestrutura de rede considera as interfaces e os caminhos de conectividade disponíveis em cada implantação, incluindo cenários com mais de uma conexão WAN.
- O SBC controla a sinalização e os fluxos de mídia na borda da solução. A organização lógica dos endereços utilizados em cada fluxo permite aplicar políticas de segurança, tratamento de NAT e ocultamento da topologia interna, de acordo com o desenho de rede adotado.
- A arquitetura da Plataforma Smartspace admite redundância entre servidores e sites. Em caso de falha, os componentes redundantes podem assumir a operação conforme a topologia configurada, preservando a continuidade das comunicações.
- As funções de firewall SIP integradas ao SBC permitem configurar regras por endereço, domínio, usuário, tronco e interconexão. A inspeção das mensagens, a limitação de tráfego e a identificação de comportamentos anômalos apoiam a detecção e o bloqueio de tentativas de registro indevidas, mensagens malformadas e ataques direcionados ao serviço de voz.
- A arquitetura de comunicação contempla sinalização SIP protegida por TLS e mídia protegida por SRTP, conforme as políticas e os parâmetros definidos para as integrações habilitadas. O SBC participa da aplicação
- das políticas de segurança dos fluxos de sinalização e mídia, incluindo os controles necessários à interconexão com redes externas e ao tratamento de cenários com tradução de endereços.
- A interconexão de voz pode ser distribuída entre pontos geograficamente separados no Brasil, hospedados em datacenters de alta disponibilidade. A plataforma também admite implantação em nuvem pública e configurações de redundância entre servidores e sites, de acordo com a arquitetura definida para cada contratação.

- As políticas de borda permitem mitigar varreduras, falsificação de origem, manipulação de mensagens, tempestades de registro e ataques de negação de serviço. Protocolos e conexões não autorizados são bloqueados conforme as regras estabelecidas.
- A plataforma rejeita conexões baseadas em versões obsoletas de SSL e utiliza conjuntos criptográficos compatíveis com a política vigente. Credenciais e segredos de integração são mantidos por mecanismos protegidos, sem exposição direta em arquivos acessíveis.
- O acesso dos usuários pode ser integrado a LDAP, Microsoft Active Directory, SAML 2.0 ou OpenID Connect. Perfis e permissões determinam as funcionalidades disponíveis para usuários administrativos, operacionais, técnicos e de suporte.
- A recuperação de acesso utiliza procedimentos controlados. Tentativas inválidas são registradas, e mecanismos de limitação, bloqueio temporário ou validação adicional podem ser aplicados para reduzir ataques de força bruta.
- A plataforma registra eventos de autenticação, configuração, administração, operação e integração. Os registros incluem identificação, data e horário e podem ser utilizados em atividades de auditoria e investigação.
- O monitoramento acompanha disponibilidade, falhas, desempenho, capacidade e utilização dos componentes. Alertas podem ser classificados por criticidade e encaminhados aos sistemas responsáveis pelo acompanhamento operacional.
- A integração com plataformas de monitoramento pode utilizar SNMPv3 com autenticação e criptografia. MIBs, traps, estatísticas e acessos de leitura podem ser disponibilizados conforme o escopo e a política de segurança aplicável.

- Os serviços em nuvem são monitorados continuamente. O dimensionamento e os mecanismos de redundância são planejados para suportar operação ininterrupta e disponibilidade mensal de 99,99%, conforme as condições previstas para o serviço.
- Ambientes organizacionais podem ser segregados em tenants independentes, com separação lógica de dados, configurações, usuários e políticas. A expansão pode incluir novas unidades e volumes sem alteração da experiência de administração.
- As APIs suportam padrões abertos de integração, incluindo REST e SOAP, com intercâmbio em JSON ou XML. A comunicação também pode utilizar HTTPS, SFTP, mensageria, filas ou streams, conforme o cenário integrado.
- As interfaces de integração possuem documentação estruturada, autenticação, proteção do transporte, controle de versões e registros de auditoria. O desempenho pode ser validado durante a homologação utilizando cenários representativos de requisições simultâneas.
- A plataforma mantém uma base consolidada de interações e registros operacionais. Dados autorizados podem ser disponibilizados por API, arquivos ou mecanismos analíticos para integração, arquivamento e geração de relatórios.
- Os registros de chamadas contêm informações de origem, destino, data, horário, duração e resultado. A retenção pode ser ajustada ao período contratual e às regras de guarda aplicáveis, com proteção de integridade e controle de acesso.
- As classes de serviço permitem estabelecer diferentes perfis de uso para ramais e usuários. As políticas podem controlar chamadas internas, locais, móveis, longa distância e internacionais, além de funcionalidades como transferência, conferência, espera e desvio.
- Categorias de uso podem variar automaticamente por horário, incluindo políticas diurnas e noturnas. Alterações administrativas permanecem registradas para consulta e auditoria.
- A identificação de origem e destino é preservada nas chamadas internas e externas sempre que fornecida pela rede participante. A plataforma também permite encaminhamento, siga-me, desvio, estacionamento, consulta, chamada em espera, conferência e não perturbe.
- O tráfego com a rede pública pode abranger chamadas fixas e móveis, locais, de longa distância nacional e internacional, conforme a cobertura e o modelo comercial contratado. Os canais são acompanhados para permitir expansão antes que a utilização comprometa a qualidade.
- A bilhetagem registra o tráfego externo e os serviços sujeitos a controle de consumo. Os relatórios podem ser organizados por unidade, ponto de conexão, ramal, destino, período e tipo de chamada.
- A portabilidade é conduzida em janelas coordenadas, com planejamento, validações, contingência e acompanhamento da ativação. O processo busca preservar o plano de numeração e as facilidades vinculadas, incluindo DDR e identificação de chamadas.
- Números adicionais podem ser incorporados ao plano de numeração em blocos organizados. Numerações especiais e curtas são tratadas conforme as condições técnicas e regulatórias aplicáveis.
- Serviços 0800 podem utilizar regras geográficas, horários, dias, origem, tipo de terminal e pontos de atendimento. As chamadas podem ser distribuídas de forma sequencial, cíclica ou percentual e redirecionadas em casos de ocupado, congestionamento ou ausência de resposta.
- As atividades de implantação são acompanhadas por gestão de mudanças, incluindo avaliação de impacto, aprovação, execução controlada e registro. A documentação do ambiente pode reunir diagramas, interconexões, configurações, produtos e visão lógica da solução.
- Materiais técnicos e operacionais podem ser fornecidos em Português ou Inglês e atualizados ao longo do ciclo contratual. O período posterior à ativação contempla acompanhamento da operação, tratamento de incidentes e ajustes de estabilização.
- Os dados são utilizados exclusivamente para as finalidades relacionadas à prestação do serviço. A proteção contempla controle de acesso, segmentação, criptografia, prevenção de vazamento, proteção contra códigos maliciosos, cópias de segurança e rastreabilidade de eventos.
- O ciclo de segurança inclui avaliações periódicas de vulnerabilidades, tratamento dos riscos identificados e comunicação de incidentes conforme a governança estabelecida. O descarte e a reutilização de mídias seguem procedimentos controlados de eliminação das informações.
- Como referências de interoperabilidade, a plataforma utiliza SIP conforme a RFC 3261, RTP/RTCP conforme a RFC 3550, SRTP conforme a RFC 3711, ICE conforme a RFC 8445, STUN conforme a RFC 8489 e TURN conforme a RFC 8656. O endereçamento telefônico observa a recomendação ITU-T E.164.
- As integrações Web podem utilizar HTTP conforme a RFC 9110, JSON conforme a RFC 8259, OAuth 2.0 conforme a RFC 6749 e JWT conforme a RFC 7519. A proteção por TLS observa as RFCs 8446 e 8996, enquanto o gerenciamento seguro pode utilizar SNMPv3 conforme as RFCs 3411 a 3418.

7 RFCs e padrões de Mercado

A Plataforma Smartspace possui suporte total a todas as RFCs detalhadas abaixo além de outras que são adicionadas à solução durante o desenvolvimento de novas funcionalidades:

- RFC 0791 - IP - Internet Protocol;
- RFC 0792 - ICMP - Internet Control Message Protocol;
- RFC 0793 - TCP - Transmission Control Protocol;
- RFC 1213 - Management Information Base for Network Management of TCP/IP-based internets: MIB-II;
- RFC 1321 - Algoritmo de hash usado para integridade de dados
- RFC 1361 - Simple Network Time Protocol (SNTP);
- RFC 1442 - Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2);
- RFC 1827 - IP Encapsulating Security Payload (ESP);
- RFC 1889 - RTP: A Transport Protocol for Real-Time Applications;
- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2246 - The TLS Protocol;
- RFC 2198 - Redundância de pacotes de áudio em RTP (VoIP resiliente)
- RFC 2327 - Session Description Protocol(SDP);
- RFC 2396 - Uniform Resource Identifiers (URI): Generic Syntax;
- RFC 2406 - IP Encapsulating Security Payload (ESP);
- RFC 2460 – IPv6 Specification;
- RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers;
- RFC 2475 - An Architecture for Differentiated Services;
- RFC 2507 - IP Header Compression;
- RFC 2543 - SIP - Session Initiation Protocol;
- RFC 2578 - Structure of Management Information Version 2 (SMIv2);
- RFC 2597 - Assured Forwarding PHB Group;
- RFC 2616 - Hypertext Transfer Protocol HTTP/1.1;
- RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication;
- RFC 2705 - Media Gateway Control Protocol (MGCP);
- RFC 2782 - Descoberta de serviços SIP via DNS
- RFC 2806 - URLs for Telephone Calls;
- RFC 2833 - RTP Payload for DTMF Digits,Telephony Tones and Telephony Signals;
- RFC 2915 – Naming Authority Pointer (NAPTR): utilizado em conjunto com SRV e DNS para descoberta de serviços SIP.
- RFC 2959 - Real-Time Transport Protocol Management Information Base;
- RFC 2976 - SIP INFO Method;
- RFC 3016 - RTP Payload Format for MPEG-4 Audio/Visual Streams;

- RFC 3047 - RTP Payload Format for ITU-T Recommendation G.722.1;
- RFC 3204 - MIME Type for ISUP and QSIG;
- RFC 3246 - An Expedited Forwarding PHB (Per-Hop Behavior);
- RFC 3260 - New Terminology and Clarifications for Diffserv;
- RFC 3261 - SIP: Session Initiation Protocol;
- RFC 3262 - Reliability of Provisional Responses in SIP;
- RFC 3263 - Session Initiation Protocol (SIP): Locating SIP Servers;
- RFC 3264 - SDP Offer/Answer Model;
- RFC 3265 - SIP-specific Event Notification;
- RFC 3266 - Support for IPv6 in Session Description Protocol (SDP);
- RFC 3267 - Real-Time Transport Protocol (RTP) Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs
- RFC 3288 - Using the Simple Object Access Protocol (SOAP) in Blocks Extensible Exchange Protocol (BEEP);
- RFC 3310 - Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA);
- RFC 3311 - SIP UPDATE Method;
- RFC 3313 – Private SIP Extensions for Media Authorization: define extensões privadas para controle de autorização de mídia em redes SIP
- RFC 3323 - SIP Privacy Mechanism;
- RFC 3324 - Identificação de chamadas em redes confiáveis
- RFC 3325 - Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks;
- RFC 3326 - The Reason Header Field for the Session Initiation Protocol (SIP);
- RFC 3327 - Registro SIP em múltiplos dispositivos
- RFC 3329 – Security Mechanism Agreement for SIP: define como negociar mecanismos de segurança para conexões SIP.
- RFC 3362 - Geração de ruído de conforto em chamadas VoIP
- RFC 3389 - Real-time Transport Protocol (RTP) Payload for Comfort Noise (CN);
- RFC 3398 - Integrated Services Digital Network (ISDN) User Part (ISUP) to Session Initiation Protocol (SIP) Mapping;
- RFC 3407 - Session Description Protocol (SDP) Simple Capability Declaration;
- RFC 3428 – IM - Instant Messaging;
- RFC 3486 – Compressing the Session Initiation Protocol (SIP): especifica compressão de mensagens SIP para redes com largura de banda limitada.
- RFC 3513 - Internet Protocol Version 6 (IPv6) Addressing Architecture;
- RFC 3515 - SIP REFER Method;
- RFC 3550 - RTP: A Transport Protocol for Real-Time Applications;
- RFC 3551 - RTP Profile for Audio and Video Conferences with Minimal Control;
- RFC 3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines;
- RFC 3581 - An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing;

- RFC 3605 - Real Time Control Protocol (RTCP) attribute in Session Description Protocol (SDP);
- RFC 3608 - Descoberta de rotas de serviço SIP
- RFC 3665 - Session Initiation Protocol (SIP) Basic Call Flow Examples;
- RFC 3666 - Session Initiation Protocol (SIP) Public Switched Telephone Network (PSTN) Call Flows;
- RFC 3680 - A Session Initiation Protocol (SIP) Event Package for Registrations;
- RFC 3688 – The IETF XML Registry: define regras para registro de nomes XML, utilizado em extensões como o SIP Event Package.
- RFC 3711 - The Secure Real-time Transport Protocol (SRTP);
- RFC 3725 - SIP Third Party Call Control;
- RFC 3840 - Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)
- RFC 3841 - Caller Preferences for the Session Initiation Protocol (SIP);
- RFC 3842 - SIP Message Waiting;
- RFC 3856 - A Presence Event Package for the Session Initiation Protocol (SIP);
- RFC 3891 - Session Initiation Protocol (SIP) "Replaces" Header;
- RFC 3892 - The Session Initiation Protocol (SIP) Referred-By Mechanism;
- RFC 3903 – SIP Extension for Event State Publication: descreve o mecanismo de publicação de eventos no contexto SIP
- RFC 3911 - The Session Initiation Protocol (SIP) "Join" Header
- RFC 3959 - The Early Session Disposition Type for the Session Initiation Protocol (SIP);
- RFC 3960 - Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP);
- RFC 3966 - The tel URI for Telephone Numbers;
- RFC 3981 - IRIS: The Internet Registry Information Service (IRIS) Core Protocol;
- RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax;
- RFC 4028 - Session Timers in SIP;
- RFC 4040 - RTP Payload Format for a 64 kbit/s Transparent Call;
- RFC 4083 - IP Multimedia Subsystem;
- RFC 4224 - RObust Header Compression (ROHC): ROHC over Channels That Can Reorder Packets;
- RFC 4235 - An INVITE-Initiated Dialog Event Package for the Session Initiation Protocol (SIP);
- RFC 4244 - Request History Information;
- RFC 4303 - IP Encapsulating Security Payload (ESP);
- RFC 4305 - Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH);
- RFC 4320 - Actions Addressing Identified Issues with the Session Initiation Protocol's (SIP) Non-INVITE Transaction;
- RFC 4346 - The Transport Layer Security (TLS) Protocol Version 1.1;
- RFC 4377 - Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks;
- RFC 4376 - Requirements for Floor Control Protocols ;
- RFC 4463 - A Media Resource Control Protocol (MRCP);

- RFC 4474 – Enhancements for Authenticated Identity Management in SIP: fornece autenticação e verificação de identidade em chamadas SIP.
- RFC 4483 – A Mechanism for Content Indirection in SIP Messages: define como referenciar conteúdos externos em mensagens SIP.
- RFC 4488 – Suppression of SIP REFER Method Implicit Subscription: trata da supressão de assinaturas implícitas no uso do método REFER.
- RFC 4497 - Interworking between the Session Initiation Protocol (SIP) and QSIG;
- RFC 4504 - Requisitos mínimos de dispositivos SIP
- RFC 4510 - Lightweight Directory Access Protocol (LDAP)
- RFC 4566 - Session Description Protocol;
- RFC 4568 - Session Description Protocol (SDP) Security Descriptions for Media Streams;
- RFC 4575 - A Session Initiation Protocol (SIP) Event Package for Conference State;
- RFC 4579 - Session Initiation Protocol (SIP) Call Control - Conferencing for User Agents;
- RFC 4582 - The Binary Floor Control Protocol;
- RFC 4694 - Number Portability Parameters for the "tel" URI;
- RFC 4733 - Telephone Events (DTMF);
- RFC 4916 - Connected Identity in the Session Initiation Protocol (SIP);
- RFC 4975 - The Message Session Relay Protocol (MSRP)
- RFC 5009 - Padronização de tipos de mídia para payloads RTP
- RFC 5168 - XML Schema for Media Control;
- RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2
- RFC 5389 - Session Traversal Utilities for NAT (STUN);
- RFC 5626 - Managing Client Initiated Connections in the Session;
- RFC 5627 - Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP);
- RFC 5766 - Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN);
- RFC 5806 - Diversion Indication in SIP;
- RFC 5850 - A Call Control and Multi-Party Usage Framework for the Session Initiation Protocol (SIP);
- RFC 5853 - SBC (Session Border Controller) for Enterprise;
- RFC 6157 - IPv6 Transition in the Session Initiation Protocol (SIP);
- RFC 6337 - Session Initiation Protocol (SIP) Usage of the Offer/Answer Model;
- RFC 6787 - Media Resource Control Protocol Version 2 (MRCPv2);
- RFC 6910 - Completion of Calls for the Session Initiation Protocol (SIP);
- RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3;

8 Informações de hardware

Todo o hardware utilizado possui homologação com a Plataforma e atende aos mais elevados padrões de qualidade, seguindo algumas especificações técnicas padrão para todos.

8.1 Especificações técnicas

- Compatível com rack padrão de 19’’;
- Suporte para até 12 E1s em um único servidor, caso as placas sejam conectadas diretamente no servidor;
- Gabinetes com dimensões de 1U ou 2U, dependendo da configuração da central;
- Interfaces E1s compatíveis com os protocolos R2 digital, ISDN e SS7, com e sem cancelamento de eco por hardware;
- Configuração de placas E1 através da interface WEB;
- Fonte redundante automática BIVOLT 100V~240V (opcional);