GESTÃO DE FRAUDES

GAC - DIRETORIA DE GOVERNANÇA, ARQUITETURA E TRANSFORMAÇÃO

JULHO / 2016

ÍNDICE

Este documento descreve a arquitetura do domínio de Gestão de Fraudes na Oi para as suas demandas de evolução a fim de orientar *demos* de sistemas para cobrir os processos relacionados ao domínio

SUMÁRIO EXECUTIVO

TOTAL DE SLIDES: 17

CONSIDERAÇÕES INICIAIS

Os seguintes pontos deverão ser observados durante este processo:

- A preparação e recepção de informações em resposta a demo em questão, sob nenhuma circunstância incorrerão em qualquer compromisso comercial e obrigação financeira para a Oi
- O Oi não assume nenhuma obrigação de reembolsar ou fazer qualquer outro tipo de remuneração a qualquer empresa especializada em resposta a este documento
- A Oi se reserva o direito de usar as informações fornecidas por empresas especializadas quando julgar apropriado
- A Oi irá possuir a propriedade intelectual de todo o material gerado internamente a partir da demo em questão
- A Oi exige confidencialidade na informação exposta neste documento e concorda em manter a confidencialidade das informações fornecidas pela empresa especializada
- As informações contidas neste documento são confidenciais e propriedade da Oi e, portanto, só deve ser utilizado para a realização da demo em questão
- O nome da Oi não deve ser utilizado como razão para promover a empresa especializada em relação à demo em questão
- O convite para as empresas especializadas para realizar a demo em questão não irá incorrer em qualquer custo para a Oi

DIRECIONADORES

Objetivos e necessidades de negócio

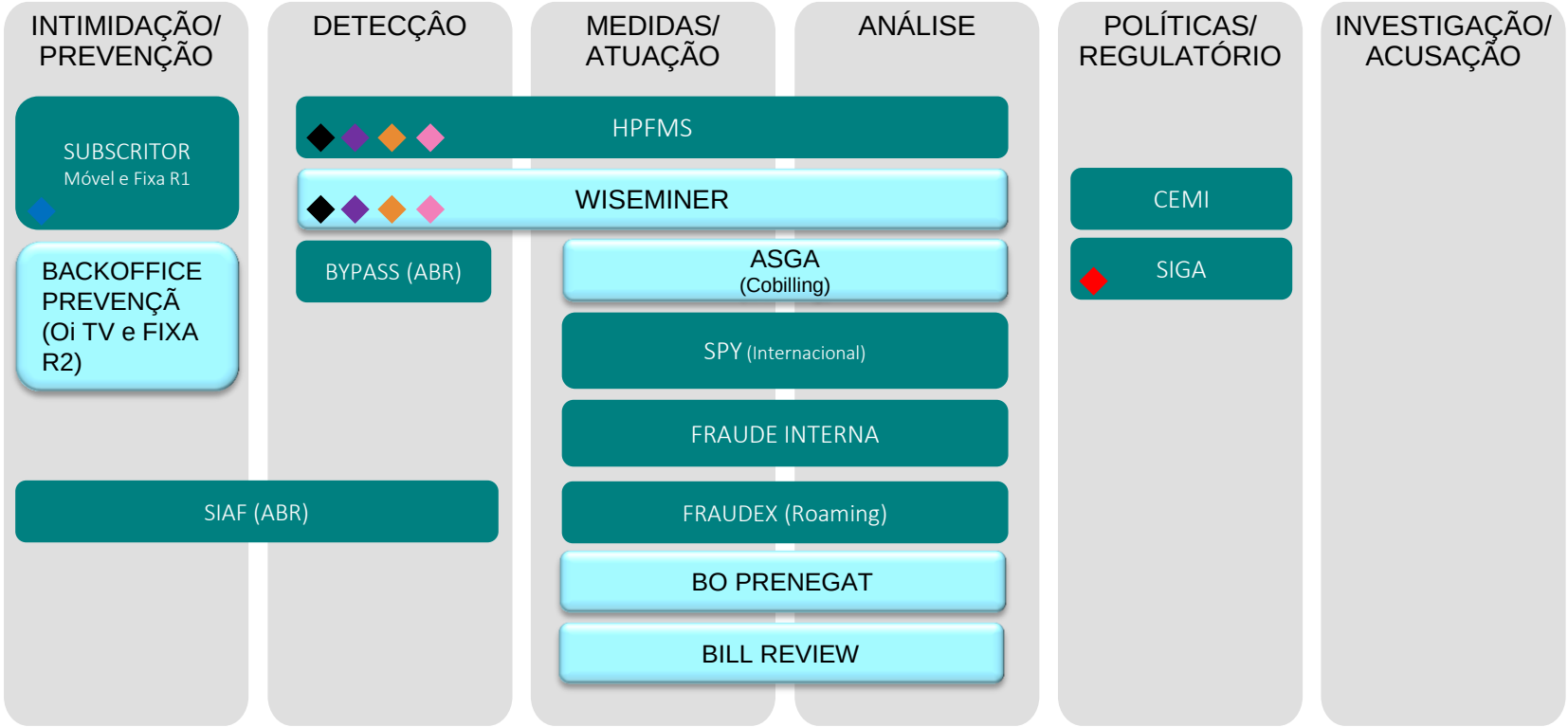
Objetivos:

- Unificar os processos de Gestão de Fraudes e habilitar as capacidades para a transformação digital na Oi

Necessidades de negócio
Preservar a experiência digital dos nossos clientes com foco também em redução de fraudes
Suprir as camadas e canais de interação digital dos nossos clientes previnindo fraudes
Monitoramento e análise da experiência do cliente em *real-time*
Suportar plataformas digitais *omni-channel* de pagamento para o cliente (credit card, pay pal, bitcoin, etc)
Real-time decision-making e novos modelos preditivos para coibição de fraudes
Detecção de padrões comportamentais através de canais digitais de interação com o cliente
Construção de modelos de detecção de atividades cybercriminais através de canais digitais de interação com o cliente
Machine learning para aplicação em métodos, algorítimos e modelos de Gestão de Fraudes

AS IS DE SISTEMAS

TI
NEGÓCIO



Tipos de fraudes:

- Clonagem
- Subscrição
- Fraude interna
- Revenda
- Pré-pago
- Roaming
- Sequestro
- VAS

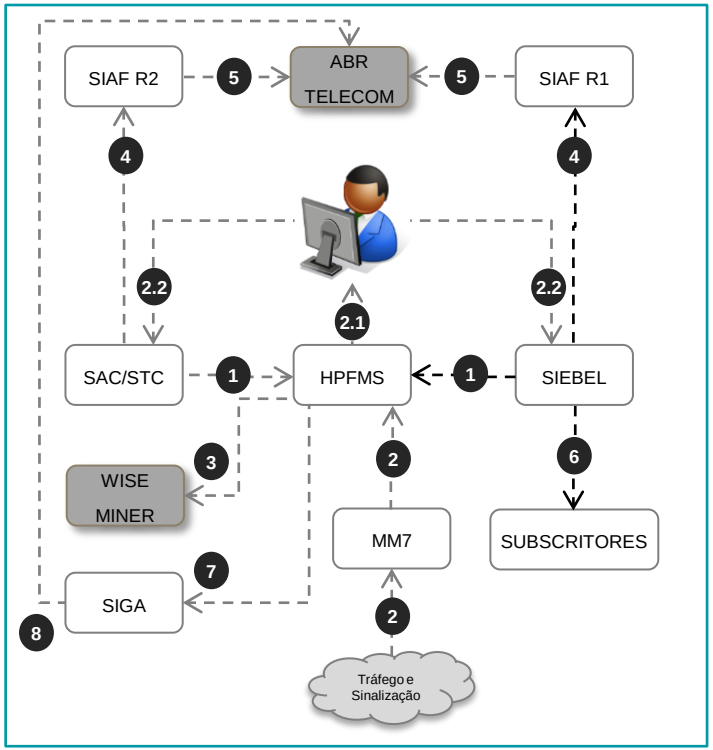
AS IS DE SISTEMAS

Estágios do ciclo de vida	Descrição
Intimidação / Prevenção	A intimidação é caracterizada pelas ações e pelas atividades destinadas a inibir ou desanimar o fraudador antes de executar a fraude, por medo das conseqüências. O possível fraudador não tentará porque as probabilidades do sucesso da fraude não são suficientemente boas. Dado que a intimidação não dissuadiu o fraudador de cometer a fraude, a prevenção pretende impedir os fraudadores de ter sucesso. A prevenção compreende atividades que tornam a execução da fraude mais difícil, endurecendo as "defesas" contra os fraudadores (por exemplo, a autenticação do aparelho)
Detecção	Conjunto de ações e de atividades, tais como sistemas antifraude, são utilizadas para identificar e encontrar a fraude antes, durante e depois da conclusão da atividade fraudulenta. A intenção da detecção é descobrir ou revelar a presença da fraude ou de uma tentativa de fraude
Medidas / Atuação	O objetivo é a tomada de medidas que evitem a ocorrência de perdas ou a sua continuidade, e ou impeçam um fraudador de continuar a fraudar ou terminar a sua atividade de fraude (por exemplo, executar a desativação de um assinante ou telefone celular)
Análise	Perdas que ocorreram apesar dos estágios precedentes, neste estágio são identificadas e estudadas para determinar os fatores em que ocorreram as fraudes
Políticas / Regulatório	Compreende o conjunto de atividades que pretendem criar, avaliar, comunicar e ajudar na implantação de políticas para reduzir a incidência da fraude. Equilibrar as políticas de redução de fraude com as restrições de orçamento e gerência eficaz é uma obrigação neste estágio
Investigação / Acusação	A investigação envolve obter evidências suficientes e informações para parar a atividade fraudulenta, para recuperar recursos ou obter a restituição dos mesmos. A Acusação bem sucedida e a condenação do fraudador dependem na maior parte da investigação. Neste estágio está clara a necessidade do suporte jurídico (leis) para condenar os criminosos

AS IS DE SISTEMAS

Tipos de fraude	Descrição
Clonagem	É a "cópia" desautorizada da identidade de um terminal para permitir que as chamadas sejam cobradas de um cliente válido. Neste cenário, os números de identificação de celulares válidos (MIN) e os números de série eletrônicos (ESN) ou IMSI (redes GSM) são obtidos na rede de telefonia celular. Estas combinações válidas de MIN/ESN podem ser adquiridas de várias maneiras, entre elas pela "escuta" nos canais do controle e de comunicação dos terminais, ou através de uma fonte interna a operadora de telefonia celular
Subscrição	A Fraude de Subscrição se caracteriza pela apresentação de informação imprecisa ou incorreta para obter um contrato de serviço ou, por outro lado, pelo não cumprimento das obrigações desse contrato. A Fraude de Subscrição ocorre quando um assinante contrata o serviço com identificação falsa ou informação fraudulenta obtida de cliente "real", e não tem nenhuma intenção de pagar pelo serviço
Fraude interna	A Fraude Interna é cometida quando um empregado da operadora ajuda na obtenção de informações, serviços opcionais, ou equipamentos que permitem que o fraudador obtenha o acesso à rede ou ao serviço sem pagar por ele
Revenda	A Fraude de Revenda pode ou não incluir a maquinação ou o conluio de um revendedor. Neste caso, as solicitações para novas linhas telefônicas são aceitas e aprovadas sem verificação apropriada da identidade ou sem informação suficiente o bastante para produzir uma conta para o assinante
Pré-pago	Fraudes em rede de pré-pago, como efetuar recarga fraudulenta de créditos, impedir a dedução do saldo da chamada, invasão ("hacking") de certos tipos de aparelhos para parar de deduzir a chamada atual do saldo, etc
Roaming	É a Fraude na qual obtêm-se telefones celulares ilegalmente ou cartões SIM adulterados (GSM) para fazer chamadas na operadora visitada. O tempo de atraso de envio de registros de chamada incentiva e aumenta seus efeitos
Sequestro	Utiliza-se de transmissores de alta potência para capturar o sinal do telefone do assinante, assim que o processo de autenticação é completado. O transmissor pirata realiza, então, as chamadas utilizando-se da característica do serviço "siga-me" (call forwarding). O assinante "real" é desconectando da chamada e não sabe que o seu telefone ainda está sendo usado
VAS	Esta Fraude consiste em aumentar desonestamente o valor devido a um fornecedor de serviço (fraudador), organizando chamadas para esse serviço. Os fraudadores ativam o serviço em seu nome e normalmente usam cartões Pré-Pagos (para se manterem anônimos) efetuando as chamadas para o número de seu serviço, as quais são faturadas de forma incorreta, ou seja, o valor da ligação é muito menor do que a tarifa do serviço paga pela operadora ao proprietário do serviço (fraudador)

AS IS DE SISTEMAS



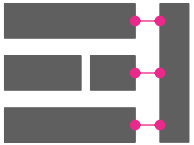
ID	Atividade	Interface
1	Extrator e envio de Cadastro	Arquivo
2	Coleta, Mediação e Entrega de tráfego e sinalização de cliente migrado	Arquivo
2.1	Análise e detecção da fraude	N/A
2.2	Cadastro da fraude no CRM	Arquivo
3	Extratores do HPFMS para o WiseMiner	Arquivo
4	Envio de cadastro e fraude para o SIAF (Antifraude Interoperadora)	Arquivo
5	Envio de cadastro e fraude para ABR Telecom (Antifraude Interoperadora)	Arquivo
6	Envio de informações de clientes	Arquivo
7	Extratores do HPFMS para o SIGA	Arquivo
8	Envio de cadastro e fraude para ABR Telecom (IMSI's)	Arquivo

PLANO DE TRABALHO

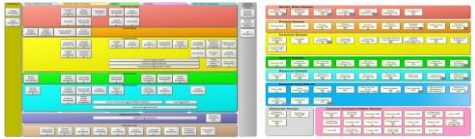
1. Statement of Work

- Metodologia
- Requerimentos
- Produtos e Casos de Uso
- Premissas e restrições
- Plano de trabalho

2. Execução



Requisitos de Arquitetura

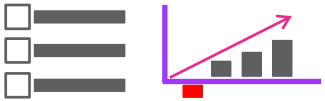


Requisitos de Aplicação e Informação

Requisitos dos Casos de Uso

3. Relatório & *Roadmap*

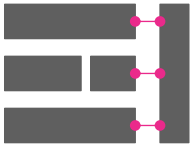
Report de Avaliação



Roadmap & *OG's*

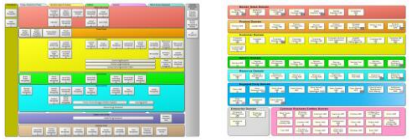
PLANO DE TRABALHO

2. Execução



Requisitos de Arquitetura

Demonstrar como solução suporta os requisitos de arquitetura. Isso deve ser feito através da demonstração de cada um dos requisitos no contexto da *demo*. O desenho das arquiteturas funcional e técnica devem ser apresentados também



Requisitos de Aplicação e Informação

Demonstrar a solução suporta os requisitos da aplicação. Isso deve ser feito através da demonstração de cada uma exigência de aplicação no contexto da *demo*. Um diagrama de entidades também deve ser apresentado para os requisitos da aplicação

Requisitos dos Casos de Uso

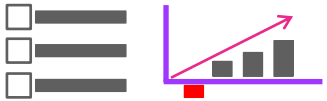
Demonstrar como a solução suporta os requisitos de casos de uso. Deve ser feito executando os passos de casos de uso no contexto da *demo*

PLANO DE TRABALHO

3. Relatório & *Roadmap*

Report de Avaliação

A Oi irá completar avaliação do fornecedor. Um relatório de avaliação vai definir o quanto o fornecedor está em conformidade com arquitetura, aplicativos, informação, produto e requisitos de casos de uso de Gestão de Fraudes



Roadmap & OG's

O fornecedor deve elaborar o *roadmap* de implementação da solução com as OG's (ordens de grandeza) de custo e prazo

REQUISITOS DE NEGÓCIO

Categoria	Descrição
Agilidade	Se antecipar a futuros *gaps* para que o FMS possa gerenciar todas as ameaças de fraude que estão sendo detectadas pelo negócio
Agilidade	Solução inovadora e flexível às exigências atuais e futuras da Oi
Agilidade	Adaptação do FMS para proteger contra ameaças atuais e emergentes
Agilidade	Flexibilidade de definições de usuário para regras e limites de alarmes
Resposta em *real-time*	Ações automáticas em tempo real para reduzir a exposição à fraudes
Resposta em *real-time*	Visão de tráfego em tempo real para descobrir padrões de fraudulentos
Resposta em *real-time*	Coletar e processar EDRs (*event data records*) em tempo real
Resposta em *real-time*	Minimizar atrasos de análise do FMS entre a conclusão da chamada e a tarifação da chamada
Assertividade	Menos falsos positivos e melhor capacidade de priorização para que os controles de fraude não impactem a experiência do cliente
Assertividade	Profundidade nas investigações de padrões quando há suspeita de fraude
Dados adicionais	Incluir clientes e dados de pagamento em tempo real
Dados adicionais	Permitir a análise das informações de fraude a partir de uma variedade de fontes, tanto internas como externas
Dados adicionais	Suporte a diversas fontes diferentes de dados, incluindo uma variedade de formatos e uma variedade de tecnologias (por exemplo, 3G, 4G, LTE, IP, etc.)
Digital Stacks	Identificar o comportamento do cliente através da sua jornada digital na Oi (mobile, web, online chat, mail, etc)

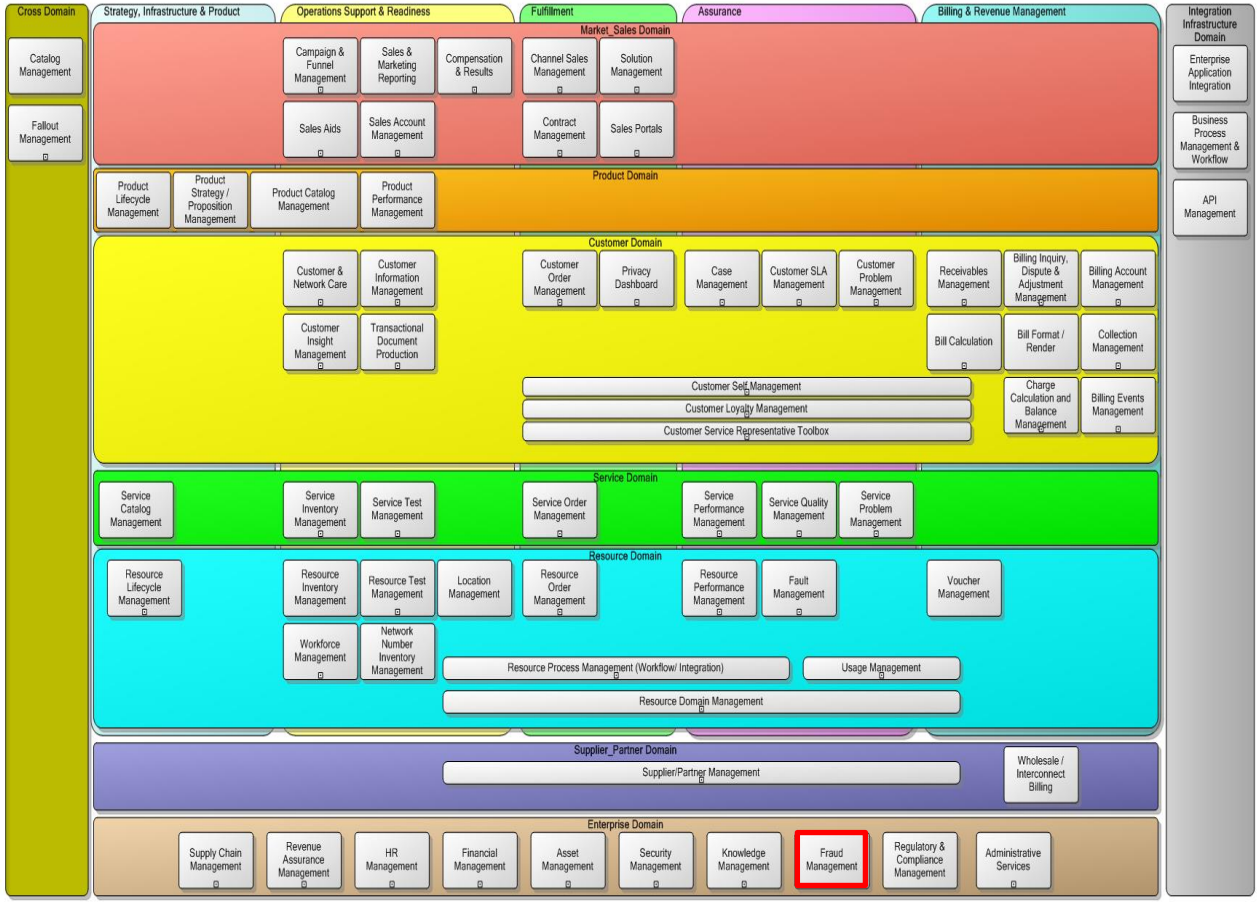
REQUISITOS FUNCIONAIS

Categoria	Descrição
Gestão da Operação	Processamento contínuo de informações e dados das normas destinadas a detectar ameaças de fraude, subsequentes da detecção de violações de suas regras
Gestão da Operação	Atividade contínua de investigar, diagnosticar e implementar controles para prevenção de fraudes, minimizando os impactos de fraude existentes
Gestão da Operação	Tomar as ações necessárias para gerenciar um problema que resultará na determinação de fraude ou não fraude
Gestão da Operação	Controlar o que acontece, operacionalmente, após a Fraude (a equipe de detectando um caso fraudulento e entregando-o para a ação corretiva)
Suporte da Operação	Identificar e combater ameaças de maneira pró-ativa e preditiva a fim de minimizar os riscos para o negócio ao se antever a uma fraude
Suporte da Operação	Gestão de Configuração do Sistema servindo como o processo de suporte para manter os dados de referência e de configuração crítica de Gestão de Fraudes
Gestão de Políticas	Estabelecer e gerenciar todas as políticas relacionadas com o emprego, uso e manutenção de ferramentas e/ou plataformas de solução utilizada na detecção de fraudes
Gestão de Políticas	Servir como um repositório de métodos e procedimentos de Gestão de Fraudes
Gestão de Políticas	Servir como um repositório para manter as melhores práticas de Gestão de Fraudes
Gestão de Políticas	Servir como um repositório para manter informações de interação com operadores internos e externos
Gestão de Políticas	Contém políticas específicas relativas à conduta de *staff* interno, e descrever o que pode ser determinada como uma violação de conduta e as penalidades associados

REQUISITOS DE ARQUITETURA

Categoria	Descrição
Apresentação	Demonstrar habilidade de interação com o cliente de forma responsiva nos canais digitais de interação (Mobile, Web, Tablet)
Apresentação	Demonstrar habilidade para configurar novas telas e workflows de navegação usando ferramentas *drag and drop*
Configuração	Demonstrar habilidade para configurar novas regras, lógicas e fluxos de negócio usando ferramentas *drag and drop*
Integração	Suportar mensagens orientadas a API's (considerando protocolos SOAP e REST), incluindo a habilidade de integrar com outras interfaces utilizando Oracle Soa Suite
Integração	Todos os serviços e integrações da solução devem ser capazes de ser monitorados, controlados e gerenciados
Infraestrutura	Demonstrar habilidade para controles de versão da solução
Infraestrutura	Demonstrar habilidade para automatizar rotinas de testes
Infraestrutura	Ser compatível com Docker para automação de *deploy*, rodando sobre servidores como Apache e Nginx (com Weblogic eJboss *application server support*)
Infraestrutura	Ser compatível com sistemas operacioanis como Linux e Red Hat
Segurança	Demonstrar habilidade para se integrar com NDS (Novel Directory Services) para Single Sign On e *user and profile management*
Dados	Demonstrar habilidade para trabalhar com dados estruturadose não estruturados (SQL and No-SQL) e permitir ferramentas externas de monitoramento de performance de *database*

DOMÍNIO DA APLICAÇÃO



Fonte: TMForum: Frameworx 15.5

- **Gestão de Fraudes**:

Investigar, prevenir e responder a atividades que indicam a utilização fraudulenta das redes ou aplicações da organização, através de sistemas de gestão de fraude eficazes juntamente com a instrumentação e monitoramento que permite atividades fraudulentas potenciais serem identificadas.

CASOS DE USO

UC 01 - *Fingerprint*

- Processamento de um cenário de tráfego de LD
- Identificação assertiva de fraude/não fraude e manutenção de base histórica
- Geração de alarmes e *dashboards* baseados no histórico de fraude por diversas tipificações

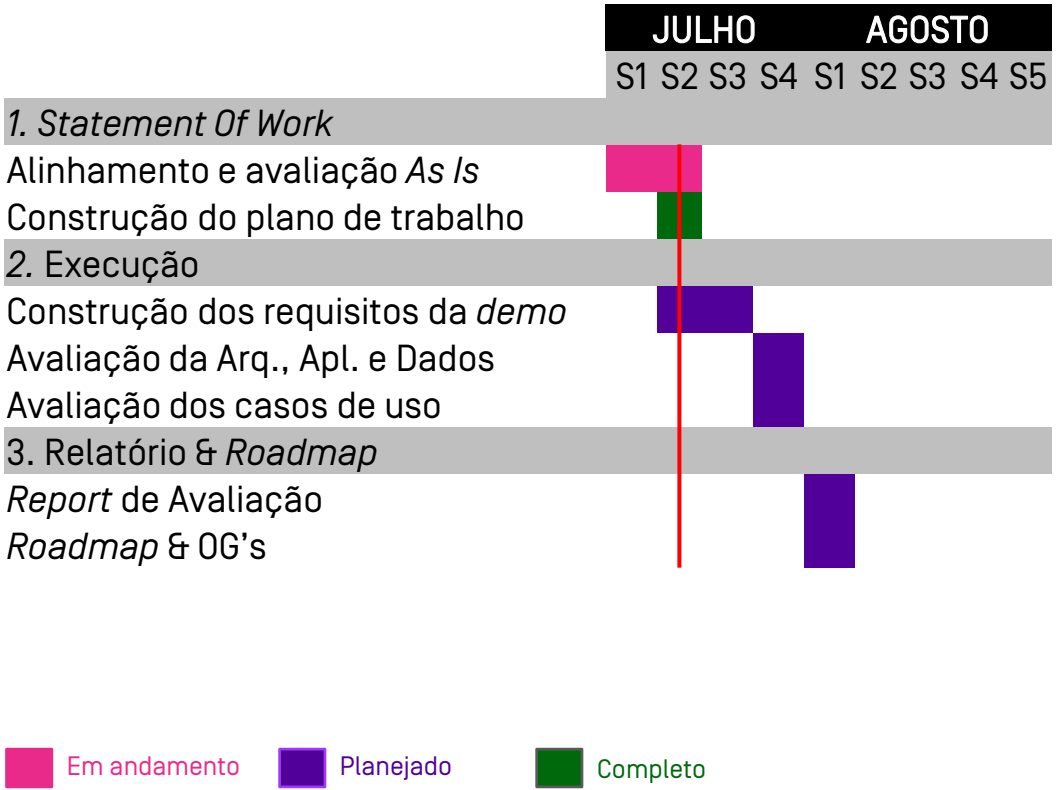
UC 02 - *Spam* pré-pago

- Processamento de um cenário de envio de vários SMS's de um mesmo assinante
- Detectar SMS's por número de terminal e por quantidade / intervalo de tempo / destinos distintos de SMS
- Geração de relatórios de uso de SMS's por diversas tipificações

UC 03 - Compra *omni-channel*

- Cliente compra um bundle em canal digital (ecommerce, mobile, etc)
- Cliente sofre análise de risco de fraude para o seu cadastro
- Possibilitar a criação de regras de acordo com a análise de risco de fraude

CRONOGRAMA


JULHO
AGOSTO
S1 S2 S3 S4 S1 S2 S3 S4 S5
1. Statement Of Work
Alinhamento e avaliação As Is
Construção do plano de trabalho
2. Execução
Construção dos requisitos da demo
Avaliação da Arq., Apl. e Dados
Avaliação dos casos de uso
3. Relatório & Roadmap
Report de Avaliação
Roadmap & OG's
Em andamento
Planejado
Completo

PREMISSAS E RESTRIÇÕES

Descrição
A integração com a arquitetura do sistema legado da Oi não é necessária. Deve ser demonstrado que a solução tem todas as capacidades de negócio técnica para suportar arquitetura, aplicação, informação e casos de uso de Gestão de Fraudes
No caso em que o fornecedor não tem todas as capacidades de negócio e técnica necessária para a solução, o fornecedor pode apresentar uma solução em parceria com outro fornecedor
Instalações de infra e internet serão fornecidas pela Oi. Porém, não é vedada a utilização de internet proprietária (modens 3G/4G, smartphones, etc)

PRÓXIMOS PASSOS

- Reunião/*call* para esclarecimentos e dúvidas - até 15/07
- Aceitação da *demo* - até 18/07


oi