

# Fênix Firewall System

Um Firewall Pessoal Sensível ao Contexto para Dispositivos  
Móveis

Marcos Alves T. de Azevedo

Instituto de Informática  
Universidade Federal de Goiás

Defesa de dissertação de mestrado, 2008

# Agenda I

# Próximos Slides

- 1 Introdução
- 2 Motivação
- 3 Justificativa
- 4 Objetivos do Trabalho

# Próximos Slides

- 1 Introdução
- 2 Motivação
- 3 Justificativa
- 4 Objetivos do Trabalho

# Próximos Slides

- 1 Introdução
- 2 Motivação
- 3 Justificativa
- 4 Objetivos do Trabalho

# Próximos Slides

- 1 Introdução
- 2 Motivação
- 3 Justificativa
- 4 Objetivos do Trabalho

# Motivação

- Engenhosidade e número crescente das ameaças virtuais. Pesquisas dizem que **83% das operadoras** de telefonia móvel no mundo foram vítimas de ataques em seus dispositivos.
- Entre os anos de **2007** para **2008** surgiram **350 tipos de malwares** diferentes para dispositivos móveis.

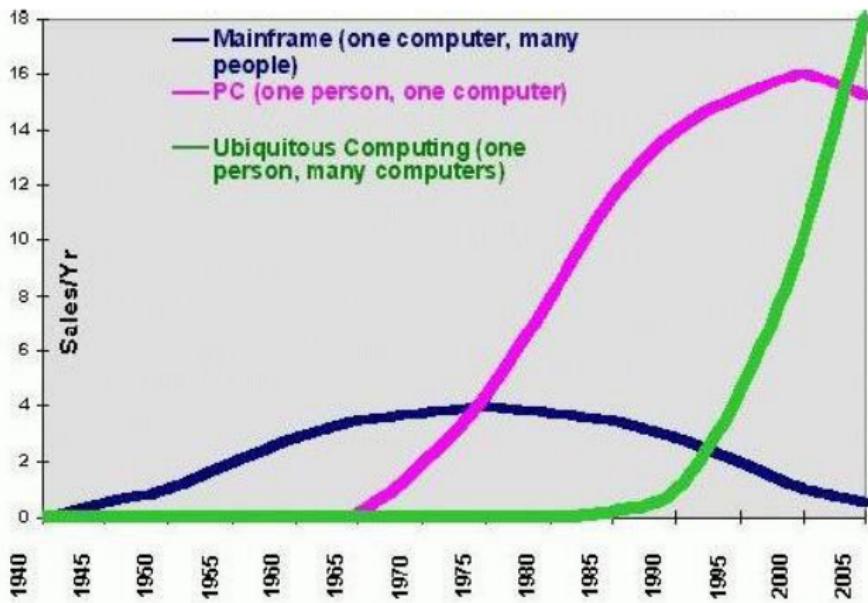
# Motivação

10<sup>a</sup> Pesquisa realizada em 2007 pela Módulo Security.

## Problemas que geraram perdas financeiras



# Motivação



## Porque usar um Firewall?

**Conectar-se à Internet sem um  
Firewall é como deixar as chaves do  
carro no contato, o motor ligado e as  
portas destravadas enquanto você  
vai às compras !**

# Porque usar um Firewall? I

- **Quanto tempo seu Dispositivo Móvel passa completamente DESLIGADO ?!**
- Redes wireless abertas tem se tornado cada vez mais comum.
- Dispositivos Móveis possuem uma variedade maior de interfaces de comunicação:
  - 1 Bluetooth;
  - 2 Wi-Fi;
  - 3 USB;
  - 4 EDGE;
  - 5 GPRS;
  - 6 Infra-vermelho

# Porque usar um Firewall?

- Imagine um Cavalo de Tróia que foi instalado junto com aquele seu toque predileto que você baixou da internet, e este Trojan envia suas senhas enquanto você acessa **E-mail e Internet Banking** do seu Dispositivo Móvel.
- Imagine que o simples fato de acessar um site através de seu Dispositivo Móvel cause o **apagamento** de todos os seus dados pessoais (Agenda, Compromissos etc)...

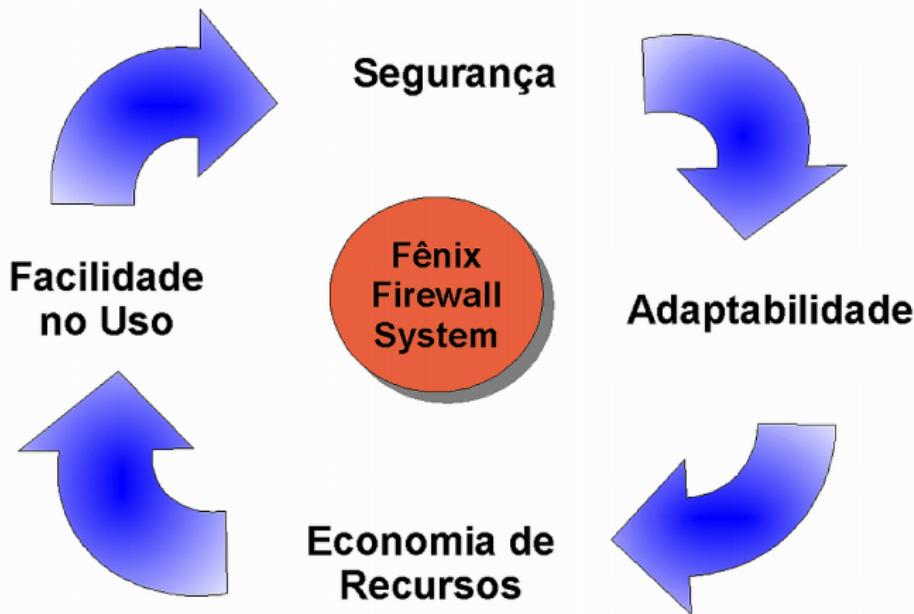
# Porque usar um Firewall?

- Imagine você esquecer o **Bluetooth** ligado e outras pessoas acessar seus dados pessoais.
- Imagine um Worm como o **Blaster** para Dispositivos Móveis, que cause uma **Negação** nos serviços de Telefonia móvel...

# Porque usar um Firewall?

- **Sem** um Firewall você está sujeito a vários ataques:
  - 1 Vírus;
  - 2 Worms;
  - 3 Cavalos de Tróia;
  - 4 SynFlood;
  - 5 Ping of Death;
  - 6 Smurf;
  - 7 Outros...

# Objetivos do Trabalho?



# Conhecendo a Fênix



## Próximos Slides

# Visão Geral da Arquitetura.

# Visão Geral da Arquitetura

## Do que o Fênix é capaz?

- **Controlar** o acesso ao dispositivo.
- **Restringir** acessos entrantes e/ou saíentes:
  - 1 Domínios (Ex.: [www.hackers.org](http://www.hackers.org));
  - 2 Redes (Ex.: 10.0.0.0/8);
  - 3 Sub-redes (Ex.: 200.137.197.129/27);
  - 4 Faixa de Endereços IP (Ex.: 172.13.0.1 - 172.13.0.10);
  - 5 Endereço IP (Ex.: 192.168.1.1/24)
- **Notificar** quando conexões suspeitas surgirem.
- **Carregar** políticas de segurança e preferências de usuário segundo a **localização**.
- **Sincronizar** e receber **notificações** de segurança com uma Plataforma Distribuída (**Opcional**).

# Ataques detectados pelo Fênix

- Varreduras de portas.
- Worms e Cavalos de Tróia.
- Ataques DoS (tradicionais).
- IP Spoofing.
- Roteamento dirigido.
- Ping O'Death.
- SYN Flood.
- Ataques contra o protocolo NETBIOS.
- Ataques contra o X-Windows.
- Ataque de Fragmentação.
- Varredura invisível.
- Transparência dos dados na rede.

# Visão Geral da Arquitetura

## Arquitetura do Fênix Firewall

### 1 **Arquitetura Embarcada.**

Instalada no Dispositivo Móvel.

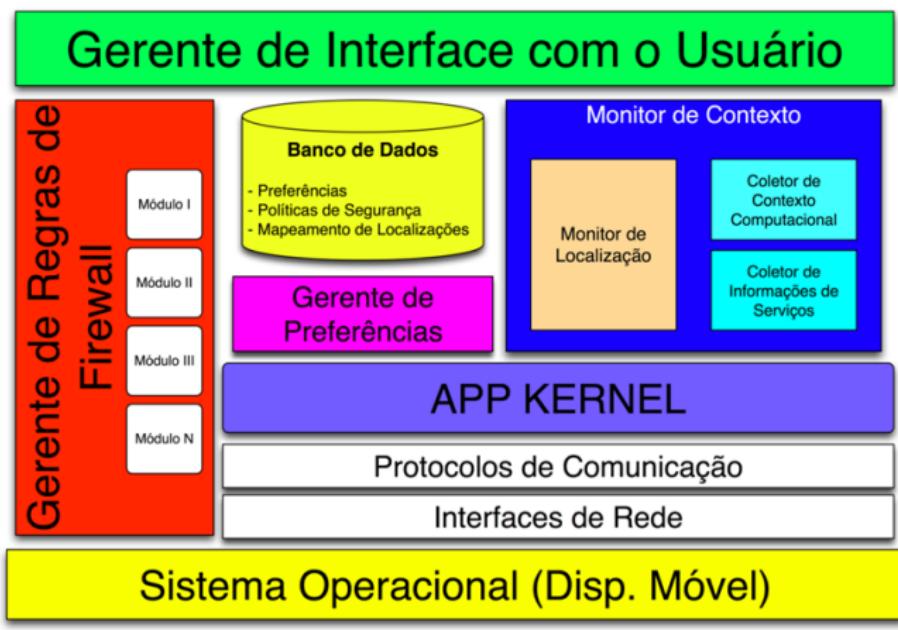
### 2 **Arquitetura Distribuída.**

Parte **Opcional**, que é instalada em computadores na WEB. Interessante para **Usuários Avançados e Terceiros.**

## Próximos Slides

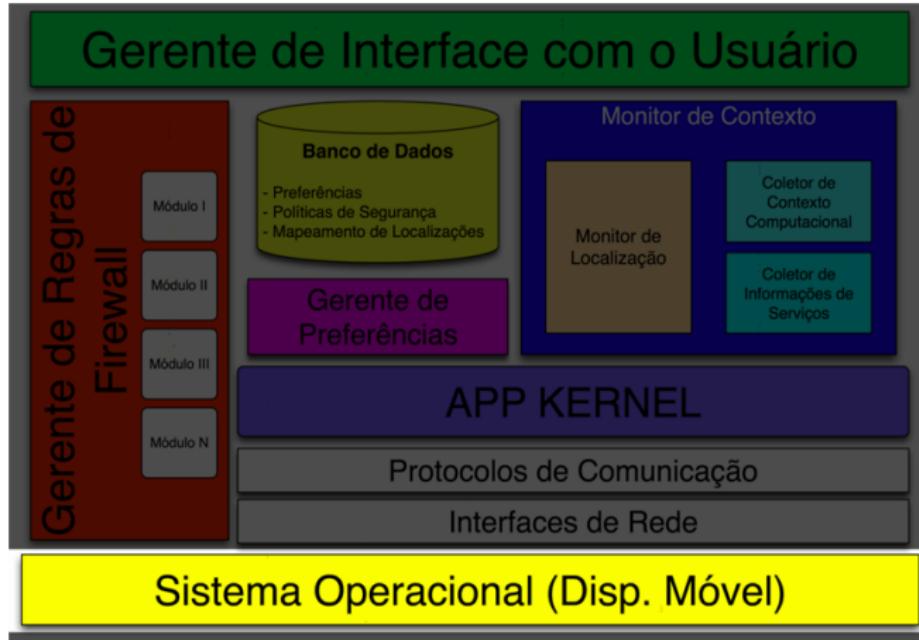
# Arquitetura Embarcada.

# Arquitetura Embarcada



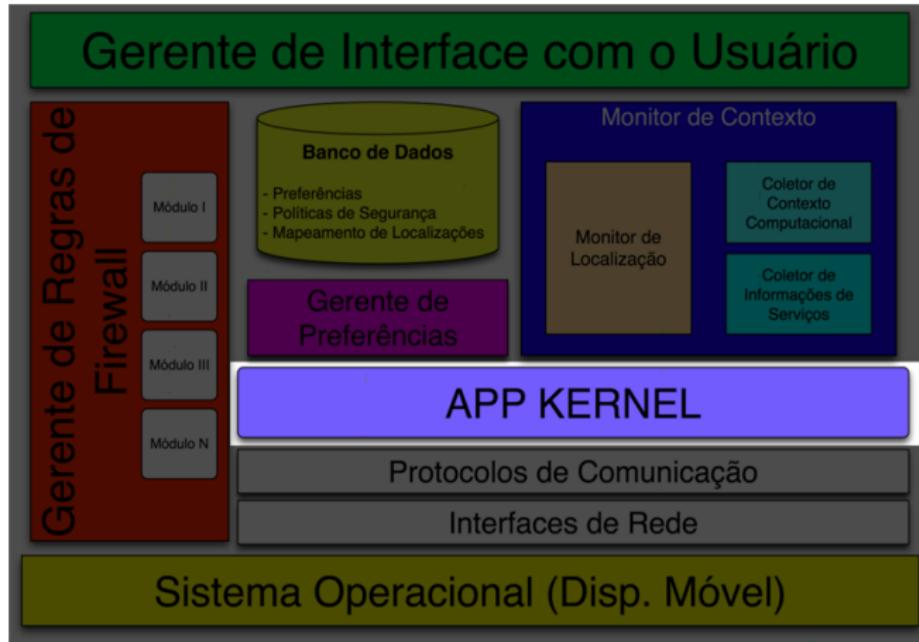
# Arquitetura Embarcada

## Sistema Operacional



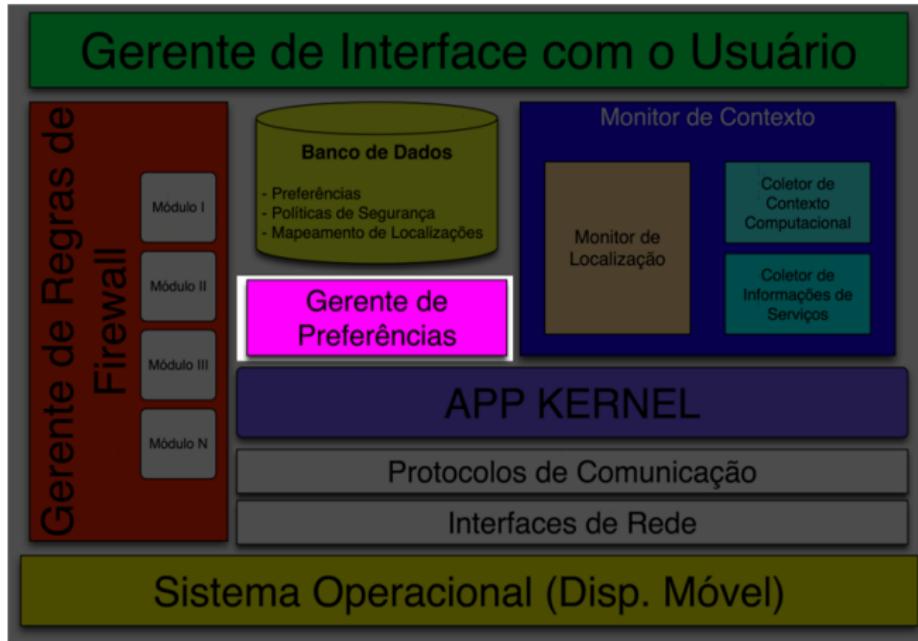
# Arquitetura Embarcada

## AppKernel (Núcleo)



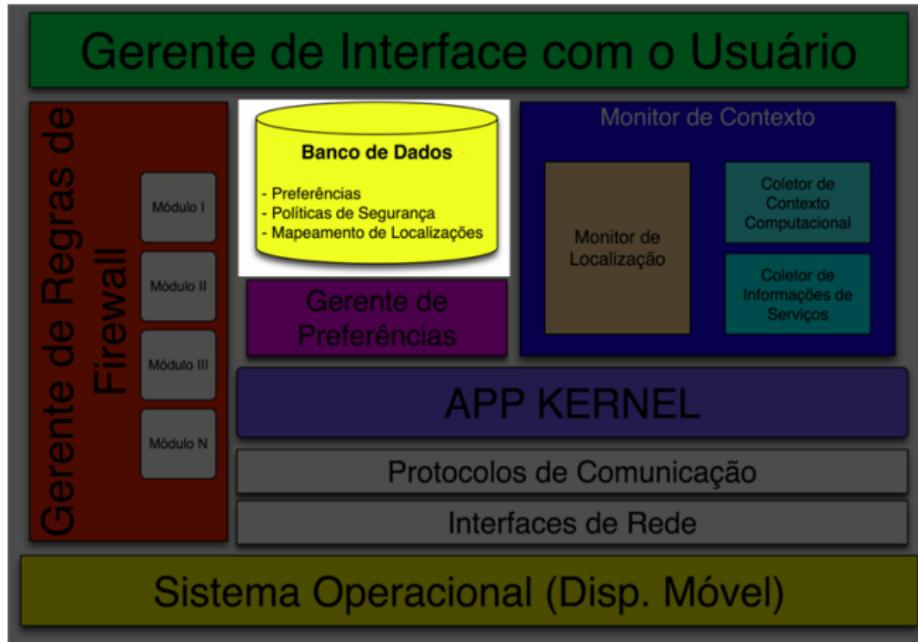
# Arquitetura Embarcada

## Gerente de Preferências



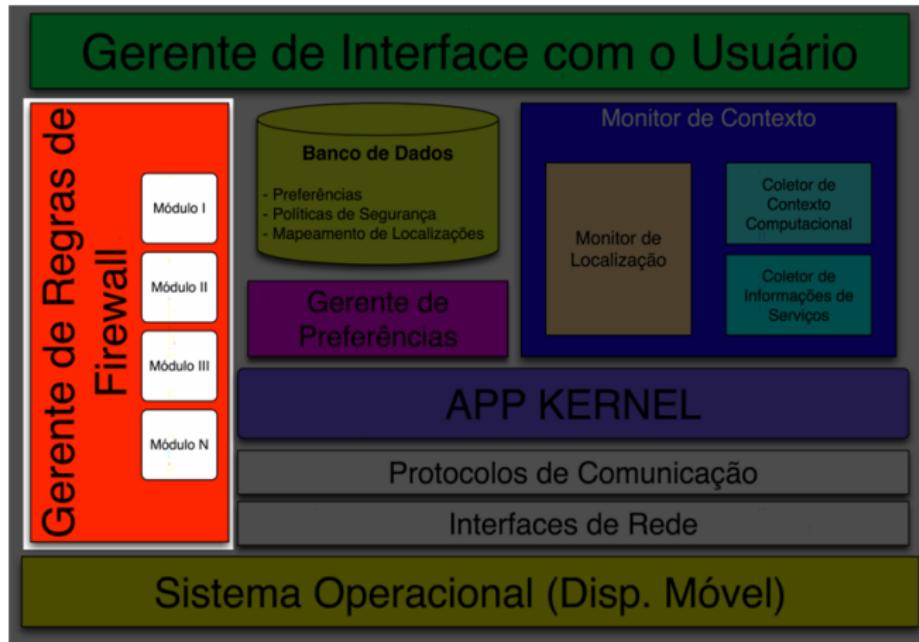
# Arquitetura Embarcada

## Banco de Dados



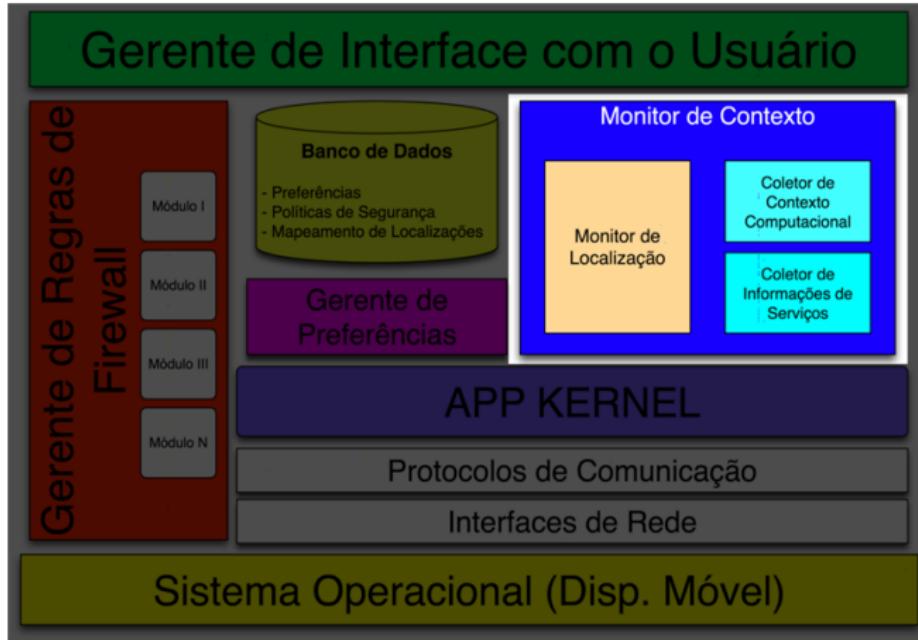
# Arquitetura Embarcada

## Gerente de Regras de Firewall



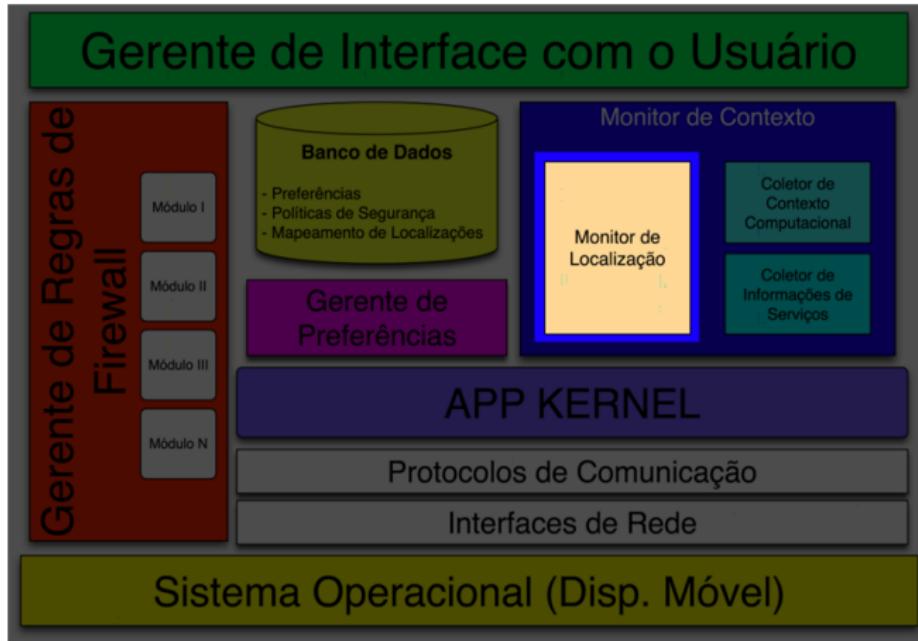
# Arquitetura Embarcada

## Monitor de Contexto



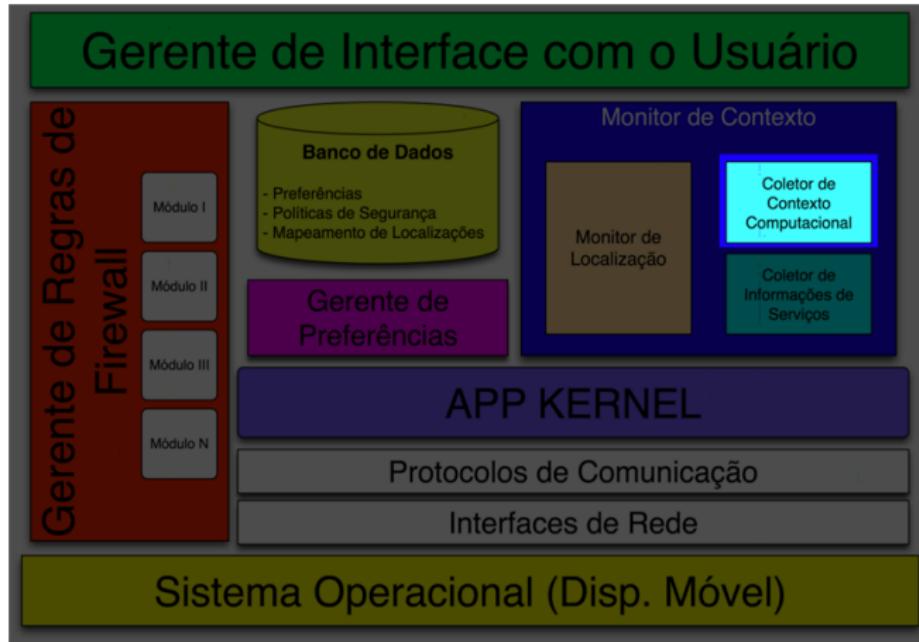
# Arquitetura Embarcada

## Monitor de Localização



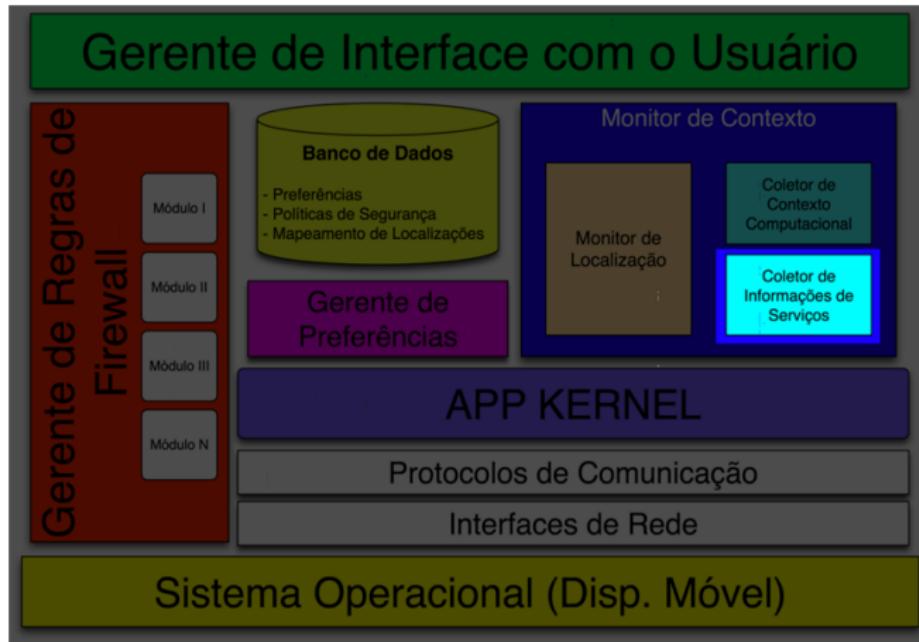
# Arquitetura Embarcada

## Coletor de Contexto Computacional



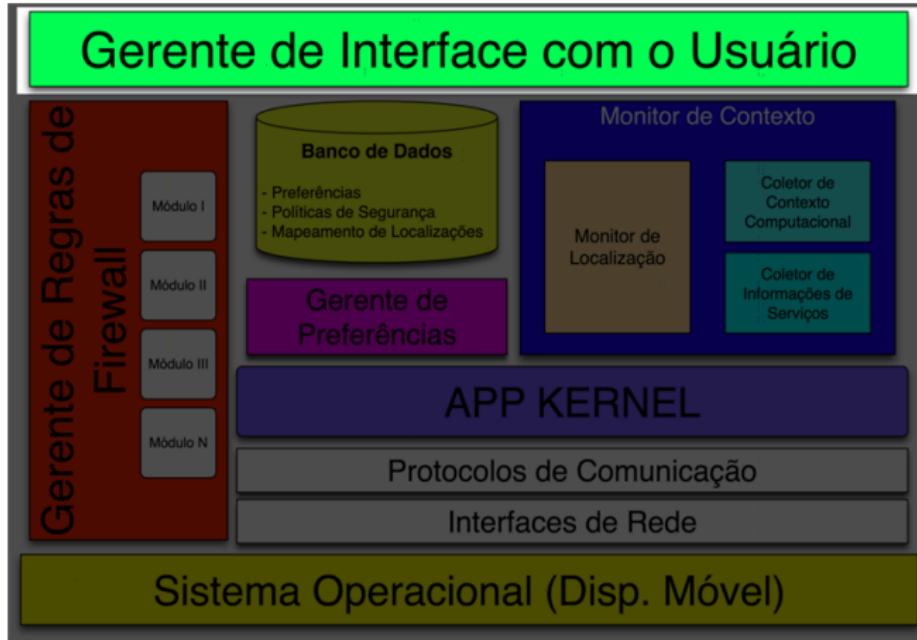
# Arquitetura Embarcada

## Coletor de Informações de Serviços

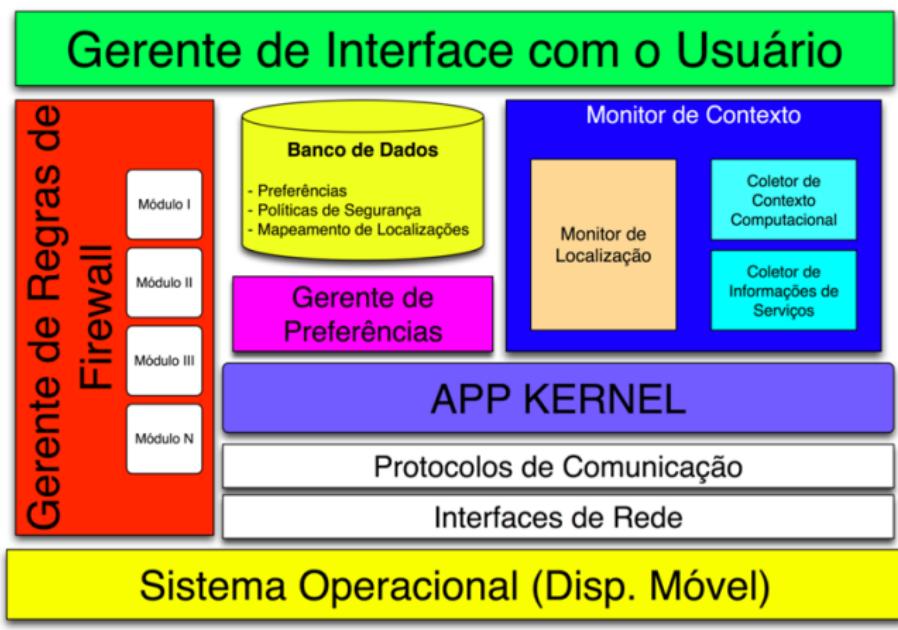


# Arquitetura Embarcada

## Gerente de Interfaces



# Arquitetura Embarcada

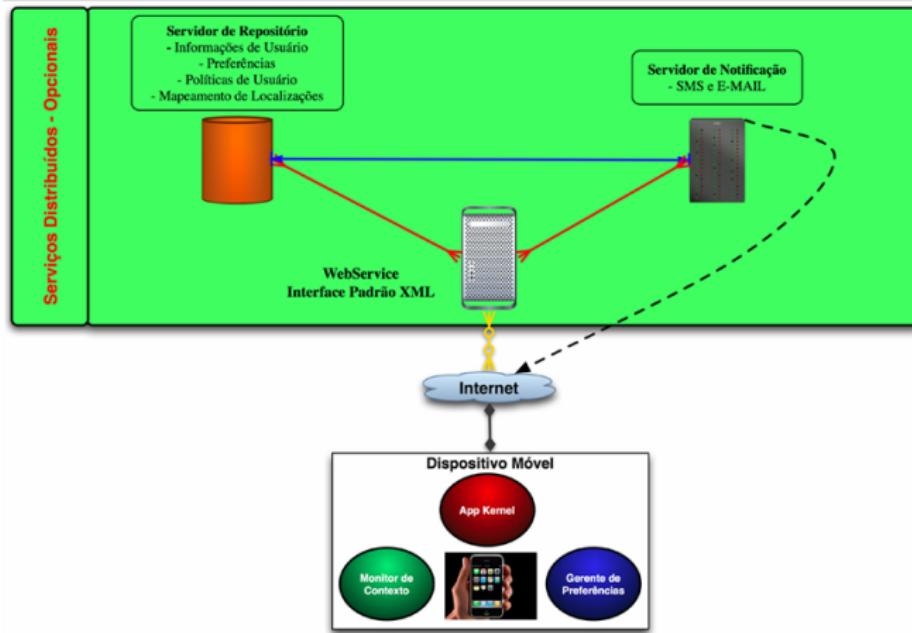


## Próximos Slides

# Arquitetura Distribuída.

# Arquitetura Distribuída

## Visão Geral



# Plataforma Distribuída (Uma **Opção** Inteligente) I

## Controle de acesso gerenciado por grupos

### 1 Administradores

Grupo de usuários com acesso privilegiado responsável pela gerência e manutenção da plataforma distribuída.

### 2 Usuários

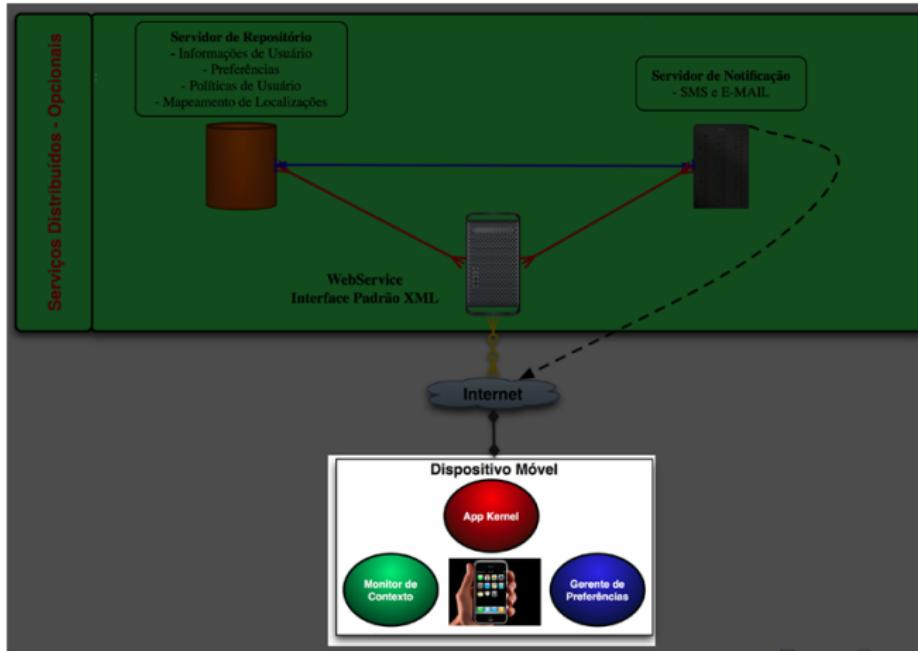
Grupo de usuários ordinários com acesso restrito á plataforma distribuída.

## Plataforma Distribuída (Uma **Opção** Inteligente) II

- Facilita **gerência** dos dispositivos móveis por **terceiros**.
- Permite maior **integração** entre os dispositivos móveis.
- Permite que o **Administrador** envie notificações importantes aos usuários.
- Permite que o **Administrador** insira uma nova política de segurança de forma autoritária, evitando ataques do tipo **0-day (Zero Day)**.
- Permite que o usuário **troque de dispositivo** e mantenha as mesmas preferências e políticas de segurança.

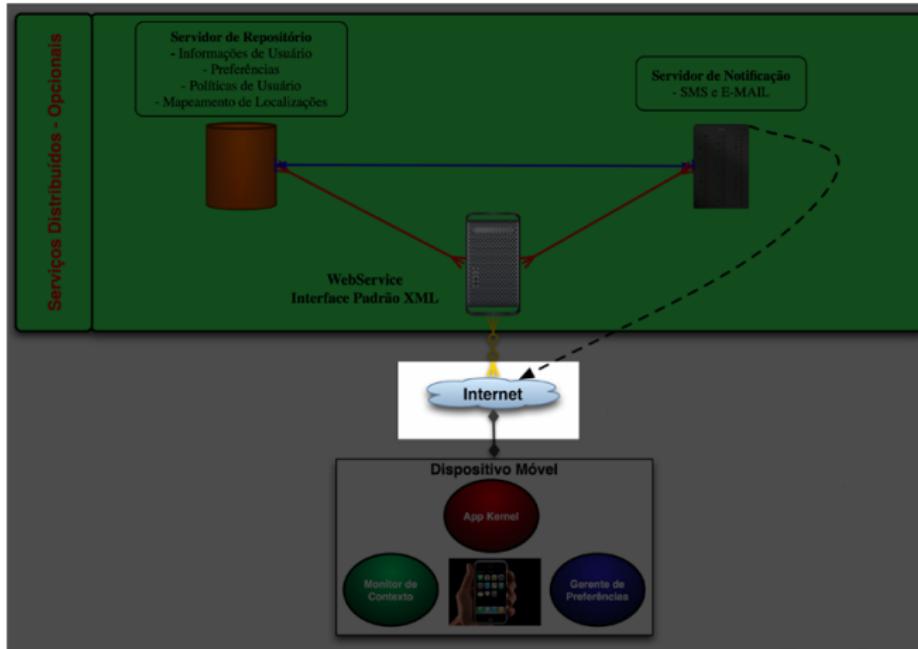
# Arquitetura Distribuída

## Dispositivo Móvel



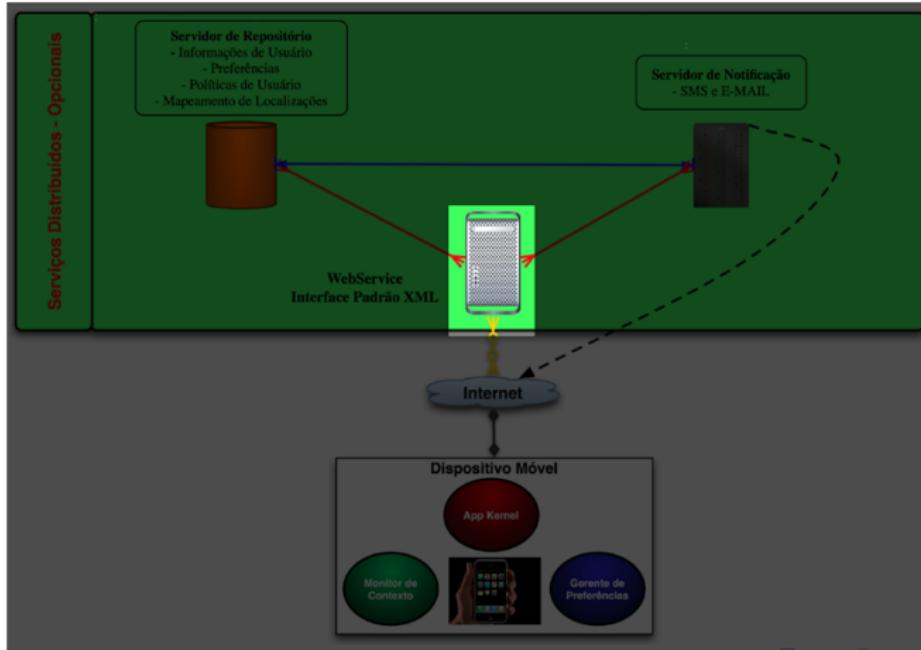
# Arquitetura Distribuída

## Conexão com a Internet



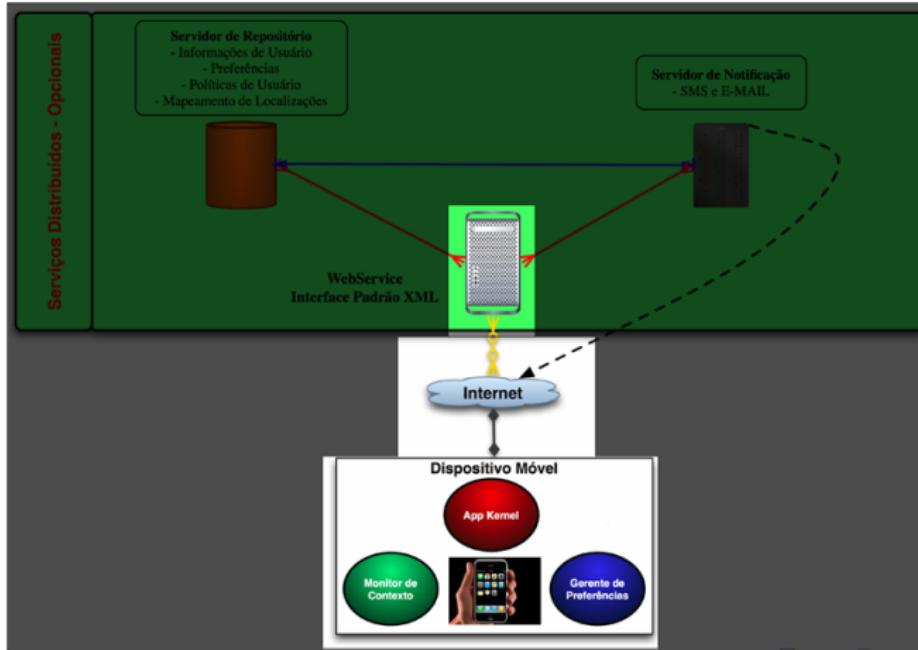
# Arquitetura Distribuída

## Servidor WebService



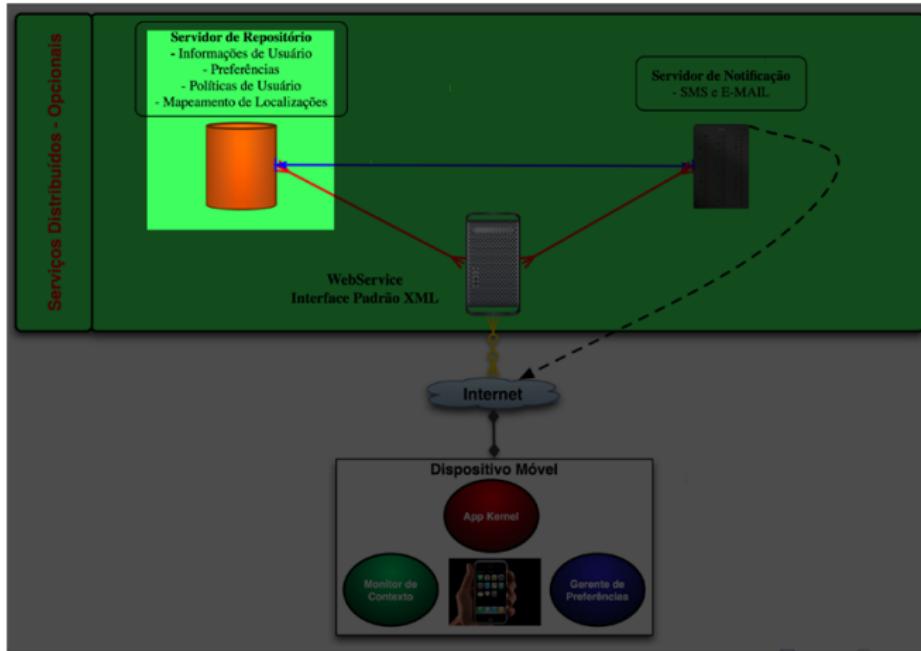
# Arquitetura Distribuída

## Conexão Disp. Móvel com Serv. WebService



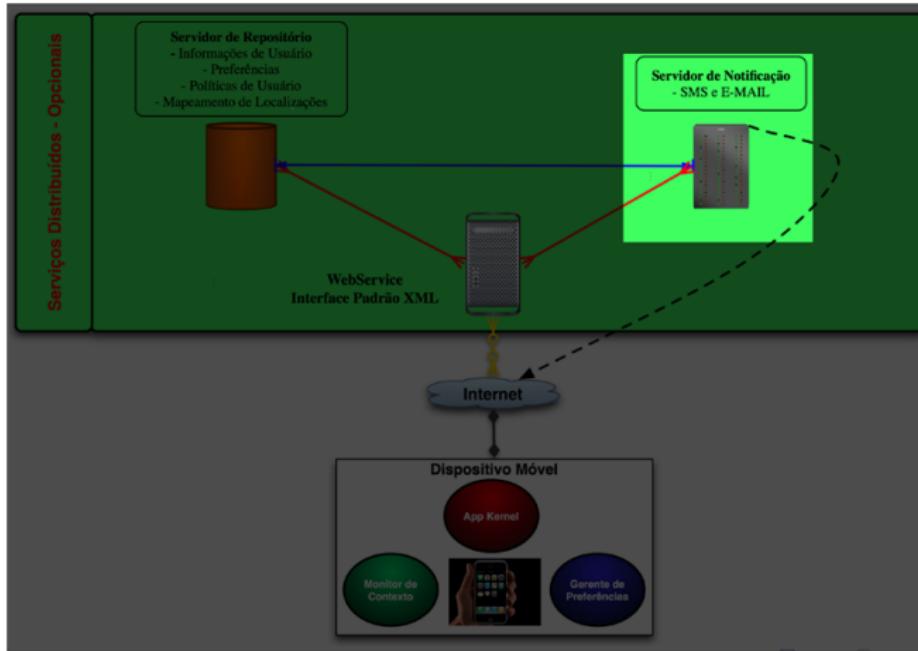
# Arquitetura Distribuída

## Servidor de Repositório



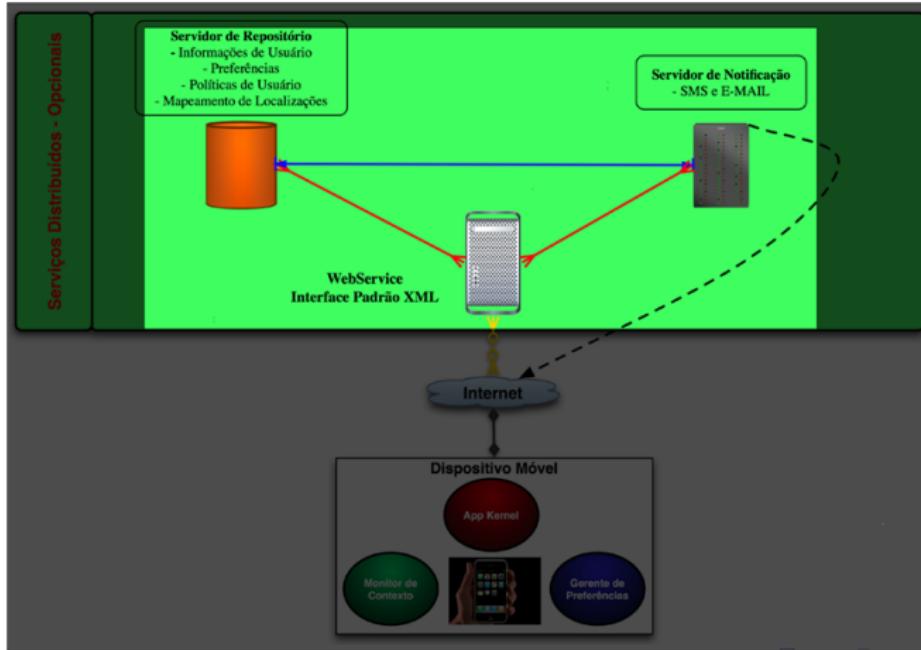
# Arquitetura Distribuída

## Servidor de Notificações



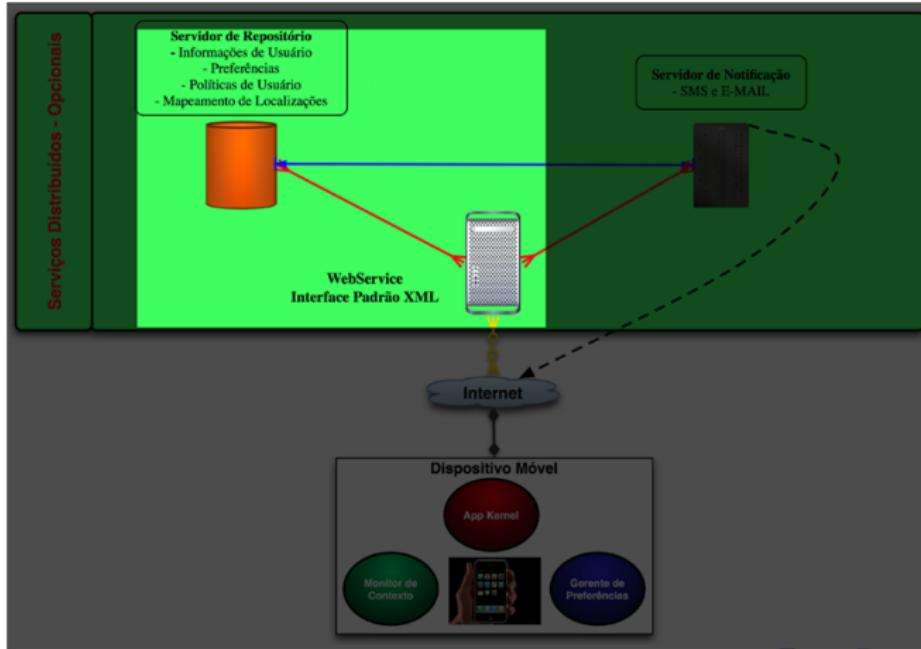
# Arquitetura Distribuída

## Comunicação entre os Servidores



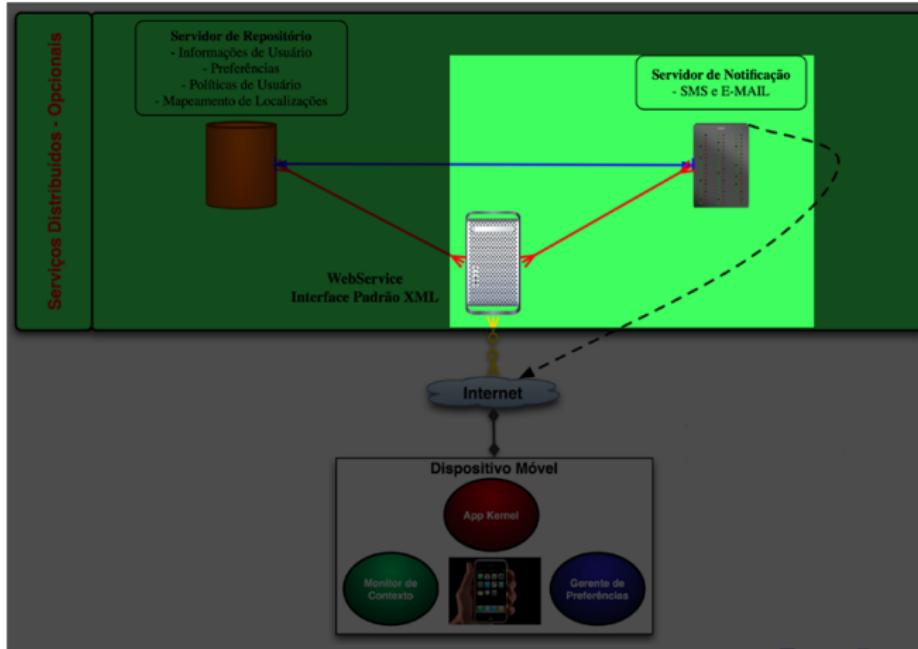
# Arquitetura Distribuída

Comunicação entre **Servidor WebService** e **Servidor Repositório**



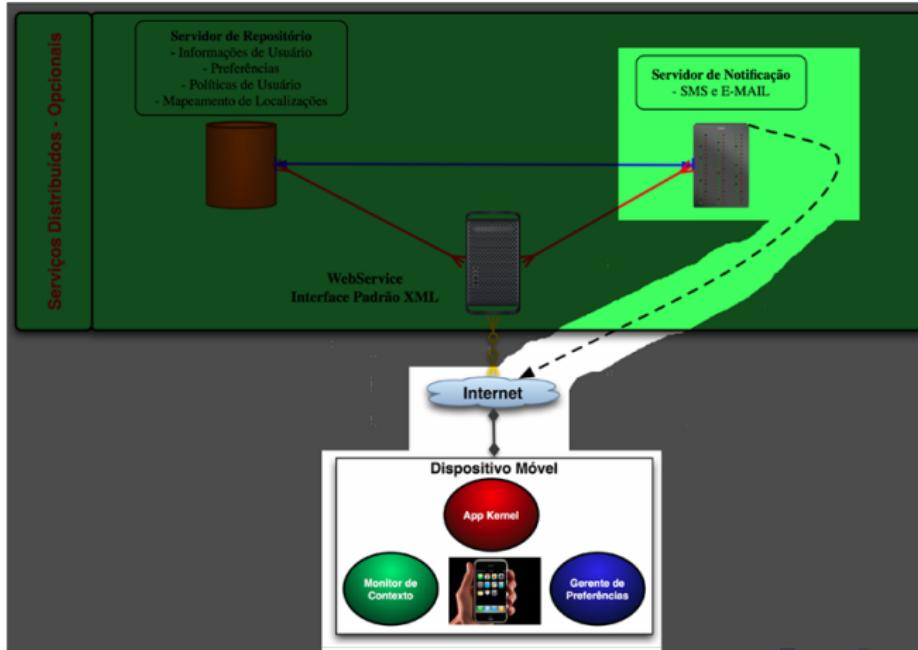
# Arquitetura Distribuída

Comunicação entre **Servidor WebService** e **Servidor Notificação**



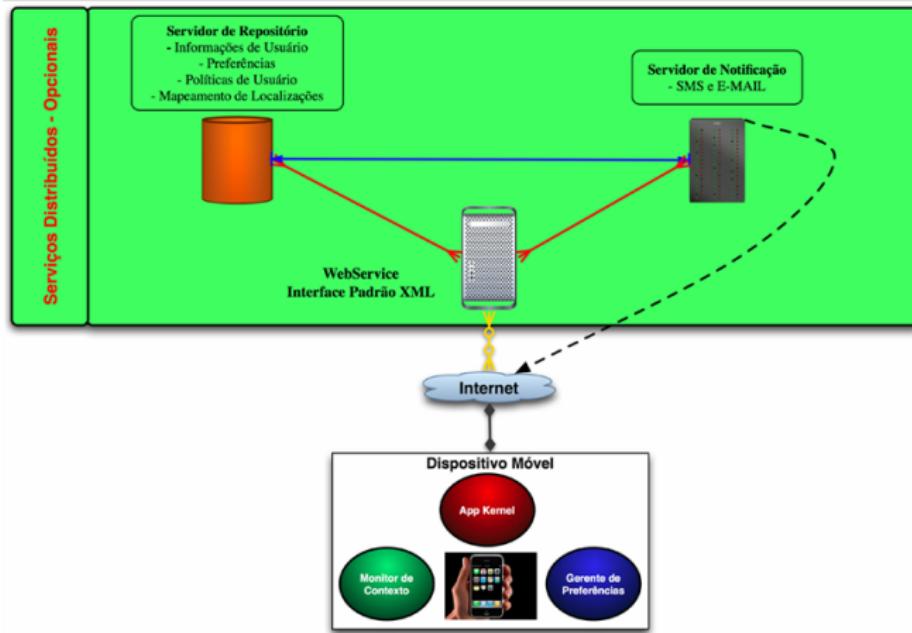
# Arquitetura Distribuída

Comunicação entre **Servidor Notificação** e **Dispositivo Móvel**



# Arquitetura Distribuída

## Visão Geral



## Próximos Slides

### Implementação da Política de Segurança Baseada em Localização.

- Identificar a Localização do Usuário.
- Mapear Áreas.
- Carregar Políticas de Segurança Baseada na Localização do Usuário.

## Próximos Slides

### Implementação da Política de Segurança Baseada em Localização.

- Identificar a Localização do Usuário.
- Mapear Áreas.
- Carregar Políticas de Segurança Baseada na Localização do Usuário.

## Próximos Slides

### Implementação da Política de Segurança Baseada em Localização.

- Identificar a Localização do Usuário.
- Mapear Áreas.
- Carregar Políticas de Segurança Baseada na Localização do Usuário.

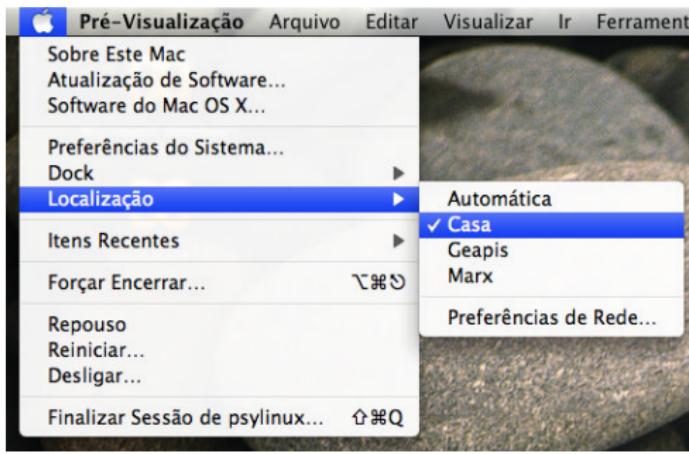
# Identificar uma Localização.

# Identificar uma Localização

Seleção Manual

## ● Forma Padrão:

- 1 Selecionar manualmente a Localização.



# Identificar uma Localização

## Seleção Automática (Opcional)

### Modos de Operação

#### 1 Ambientes Outdoor:

- Usando o recurso **GPS** presente no dispositivo, caso exista.

#### 2 Ambientes Indoor:

- Usando os recursos de **Localização** oferecido pela **Arquitetura Distribuída**.

# GPS: Identificar uma Localização.

## Consulta GPS

```
Local ← raiz[(x2 – x1)2 + (y2 – y1)2];  
se Local ⊆ banco.mapeamentos então  
    Selezione banco.mapeamento;  
    Carregue banco.politicas[Local];  
    Carregue banco.preferencias[Local];  
fim
```

## Próximos Slides

# Mapear uma Área.

# Mapear uma Área (Introdução)

**Discutiremos agora as abordagens de mapeamento relacionada aos tópicos abaixo:**

- Tipos de Mapeamento:
  - 1 Indoor.
  - 2 Outdoor.
- O que é um mapeamento.
- Formas de mapeamento.

# Mapear uma Área (Introdução)

**Discutiremos agora as abordagens de mapeamento relacionada aos tópicos abaixo:**

- Tipos de Mapeamento:
  - 1 Indoor.
  - 2 Outdoor.
- O que é um mapeamento.
- Formas de mapeamento.

# Mapear uma Área (Introdução)

**Discutiremos agora as abordagens de mapeamento relacionada aos tópicos abaixo:**

- Tipos de Mapeamento:
  - 1 Indoor.
  - 2 Outdoor.
- O que é um mapeamento.
- Formas de mapeamento.

# Mapear uma Área (Introdução)

**Discutiremos agora as abordagens de mapeamento relacionada aos tópicos abaixo:**

- Tipos de Mapeamento:
  - 1 Indoor.
  - 2 Outdoor.
- O que é um mapeamento.
- Formas de mapeamento.

# Mapear uma Área (Introdução)

**Discutiremos agora as abordagens de mapeamento relacionada aos tópicos abaixo:**

- Tipos de Mapeamento:
  - 1 Indoor.
  - 2 Outdoor.
- O que é um mapeamento.
- Formas de mapeamento.

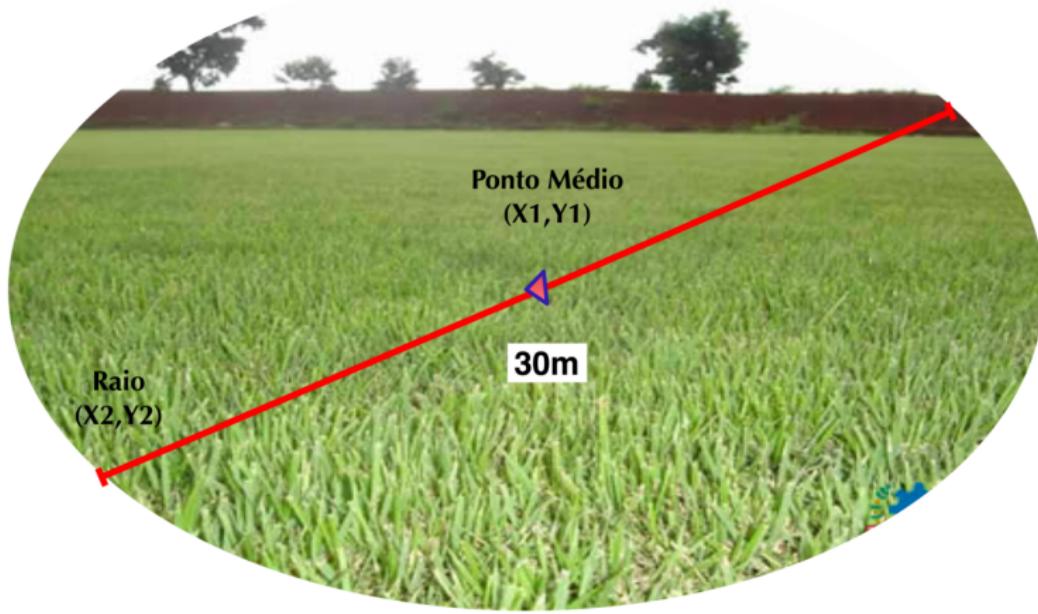
# Mapear uma Área

- Com a plataforma distribuída o grupo **Administrador** é capaz de mapear áreas comuns aos usuários.

## Tipos de Mapeamento

- 1 As áreas comuns são definidas **exclusivamente** pelos administradores, e poderão ser utilizadas por todos os usuários, ex.: *Laboratório de Redes, Secretaria, Almoxarifado*.
- 2 As áreas pessoais serão mapeadas pelo próprio usuário, e as mesmas não são visíveis ou compartilhadas para os outros usuários da plataforma.

# Política de Segurança Baseada em Localização



# GPS: Mapear uma Área

## Consulta GPS

*Local*  $\leftarrow$  raiz[ $(x2 - x1)^2 + (y2 - y1)^2$ ];

**se** *não* (*Local*  $\subseteq$  *banco.mapeamentos*) **então**

*distancia*  $\leftarrow$  raiz[ $(x1 - x2)^2 + (y1 - y2)^2$ ];

*centro*  $\leftarrow$  *distancia*/2;

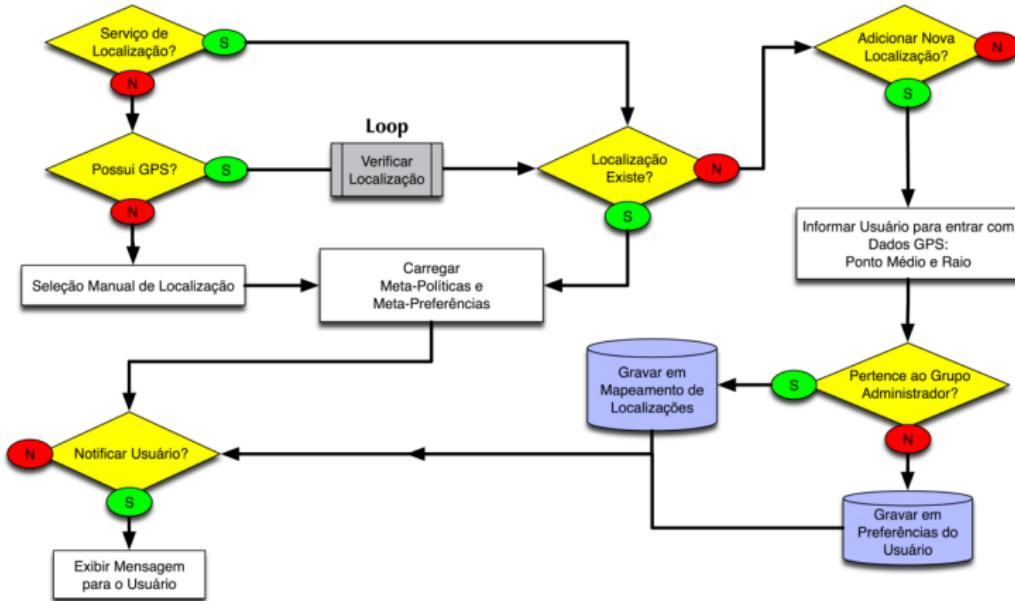
*area*  $\leftarrow$  2x*Pix*(*centro*)<sup>2</sup>;

**Escreve** Entre com a Identificação para esta localização;

**Salva Local;**

**fim**

# Política de Segurança Baseada em Localização

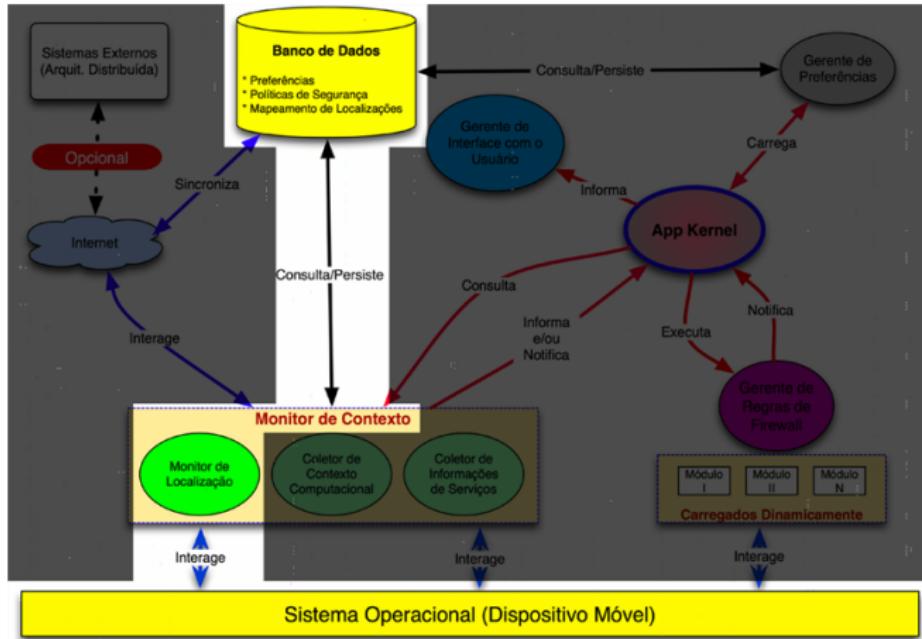


## Próximos Slides

# Ilustrando o Funcionamento.

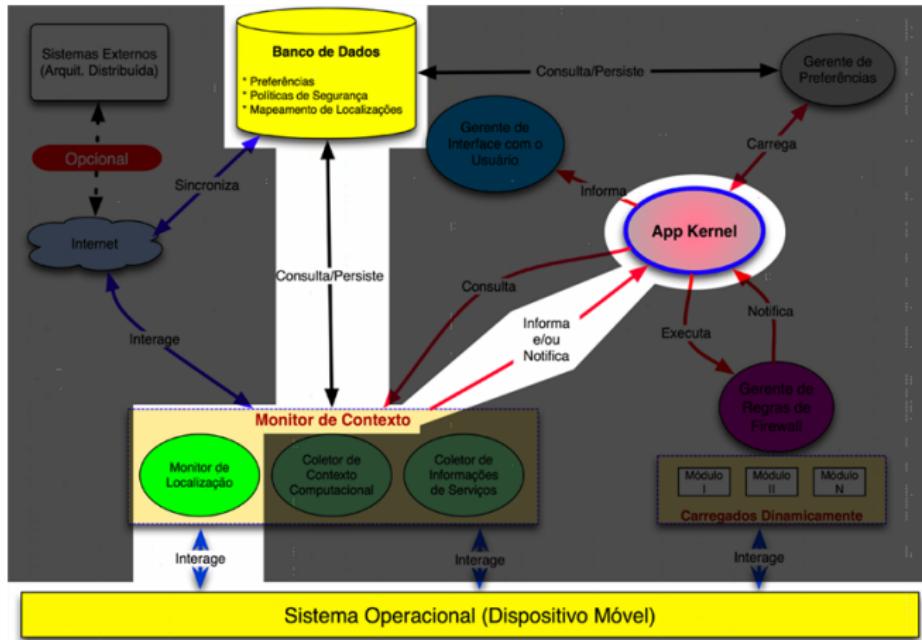
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



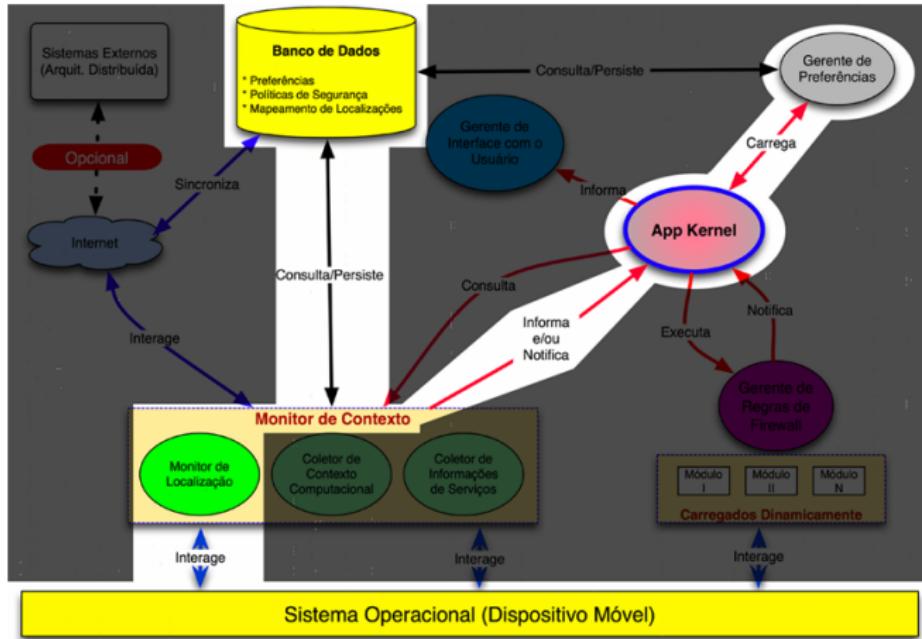
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



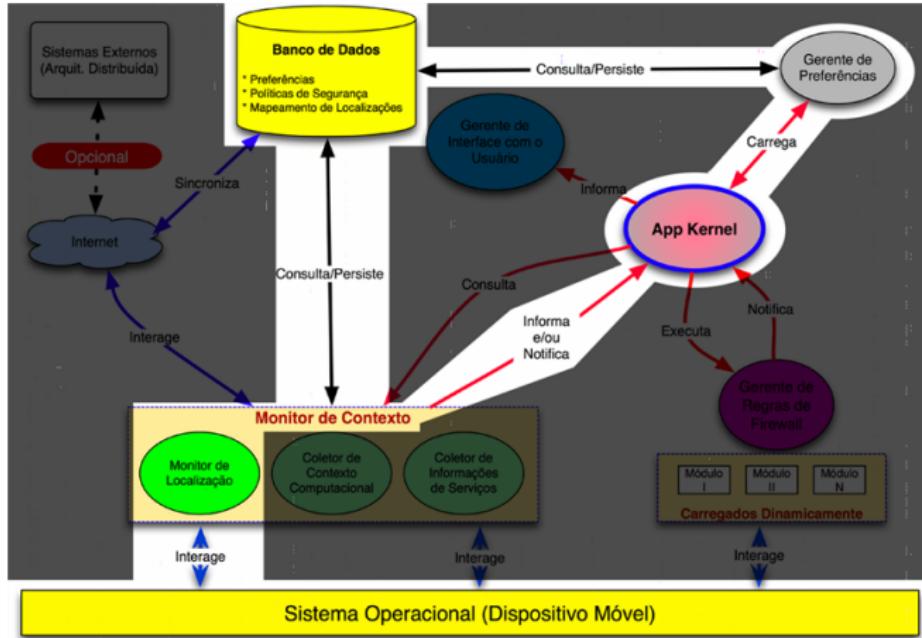
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



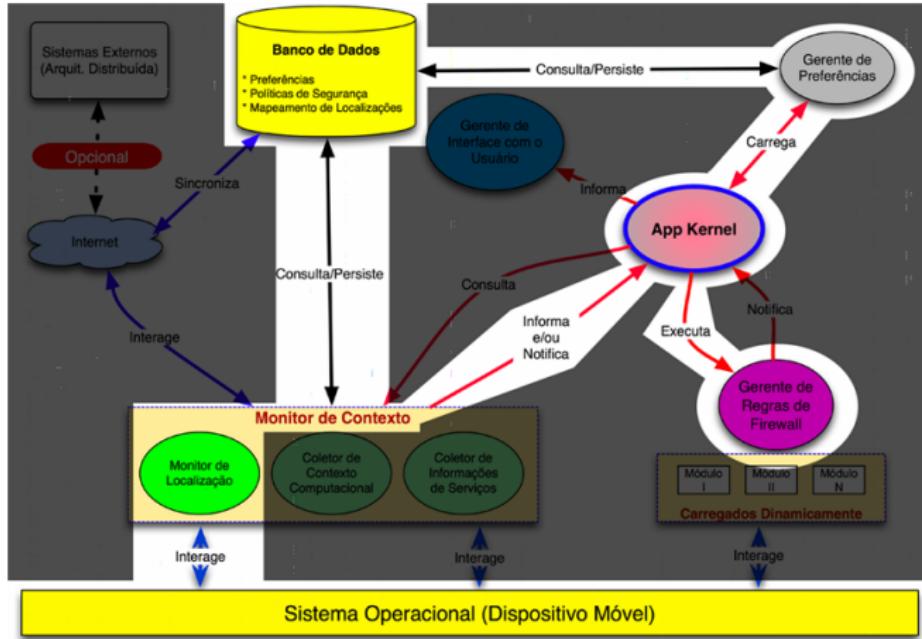
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



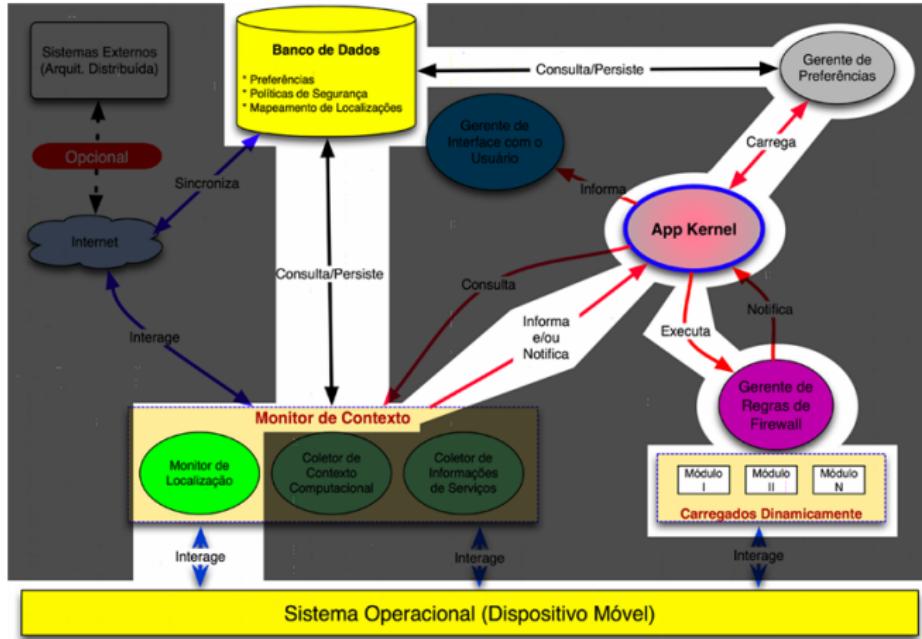
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



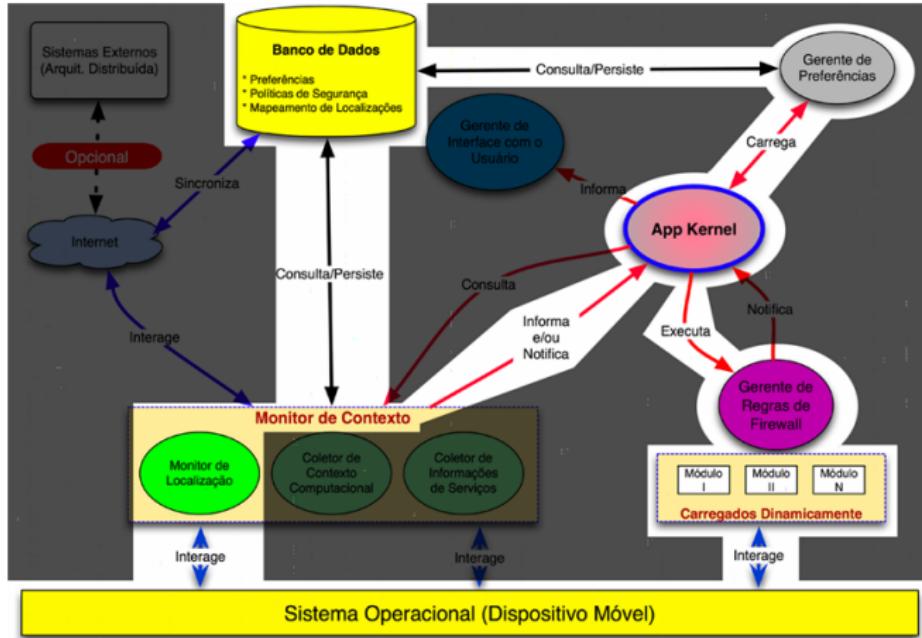
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



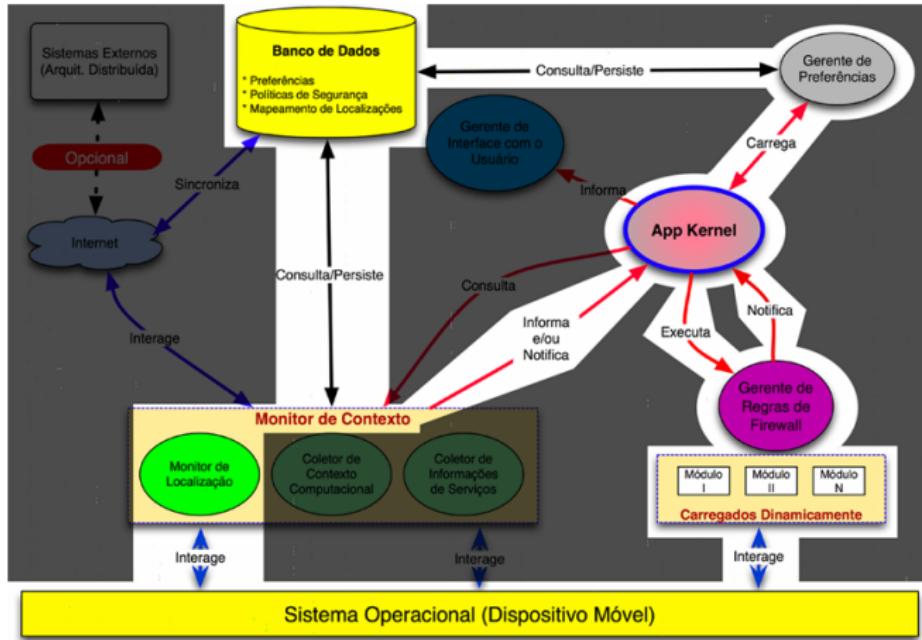
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências



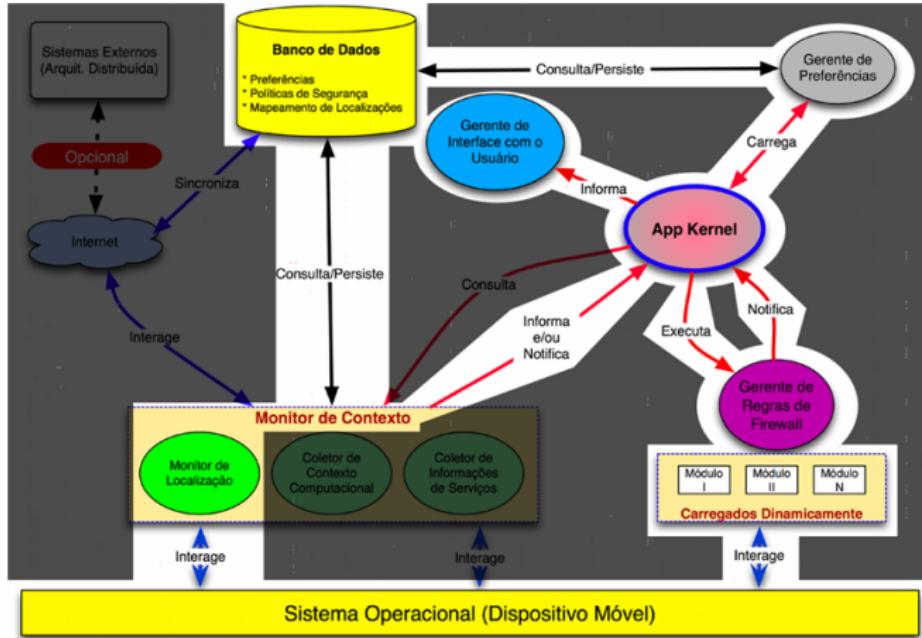
# Dispositivo Móvel com GPS

## Carregando Meta-Políticas e Meta-Preferências

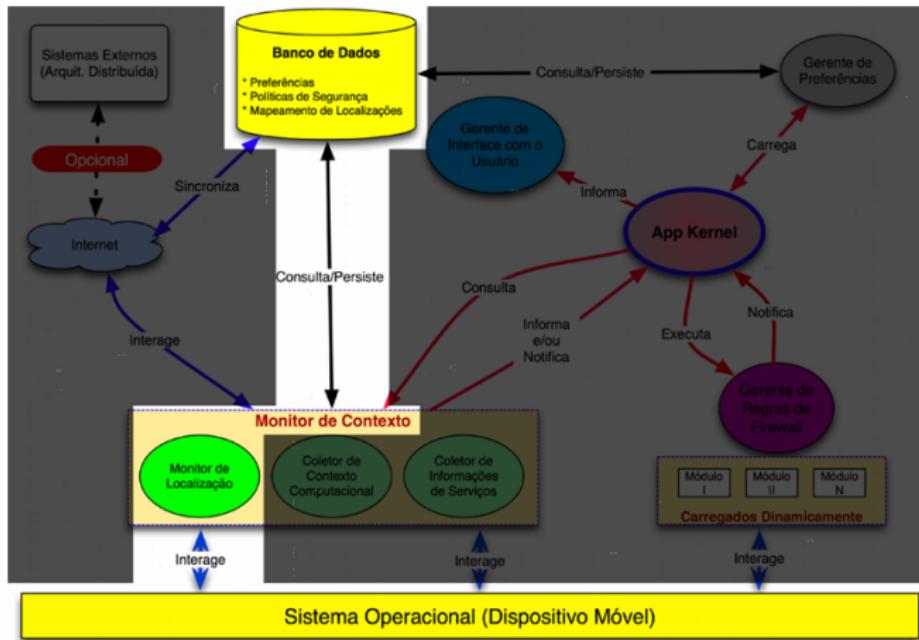


# Dispositivo Móvel com GPS

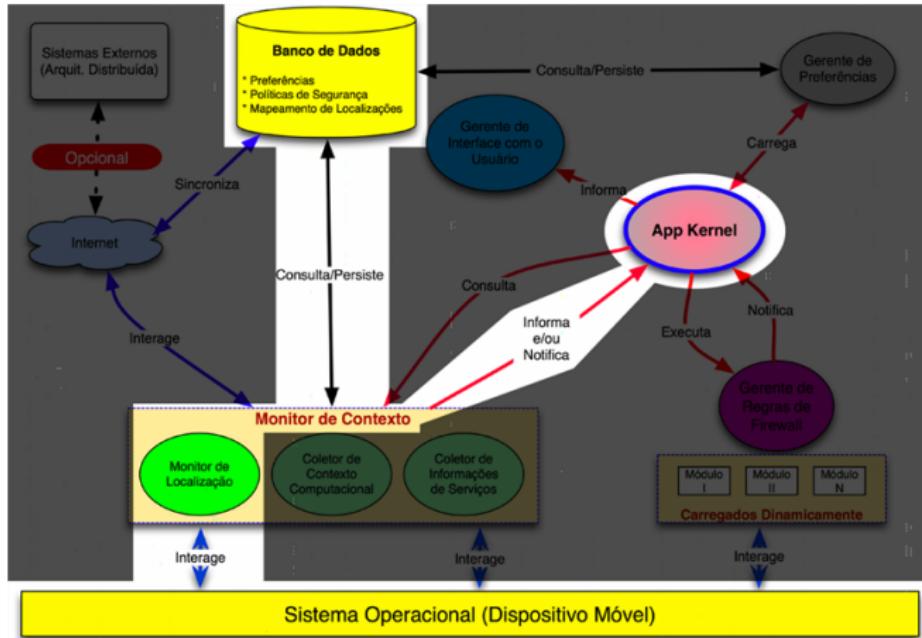
## Carregando Meta-Políticas e Meta-Preferências



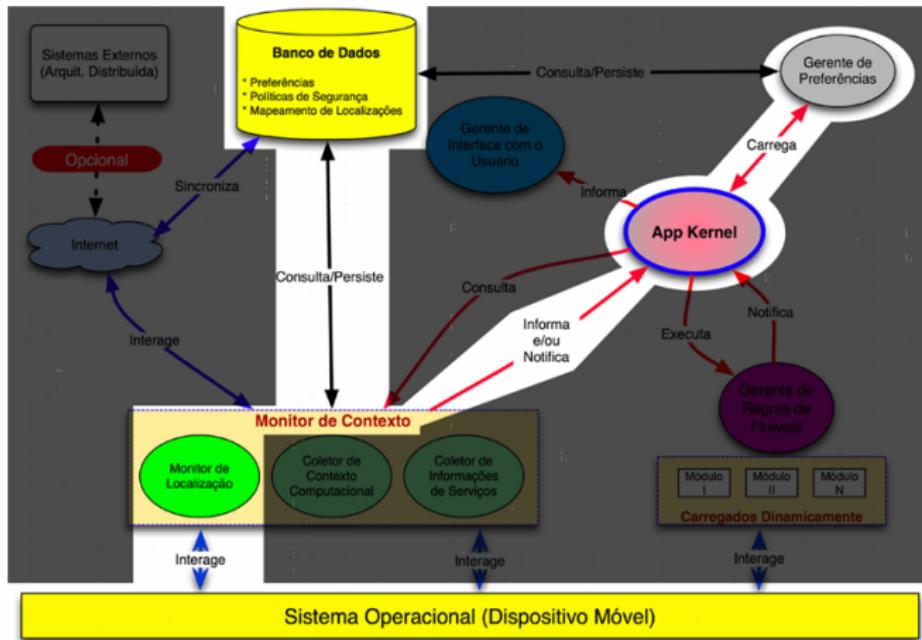
# Controlando Interfaces de Rede



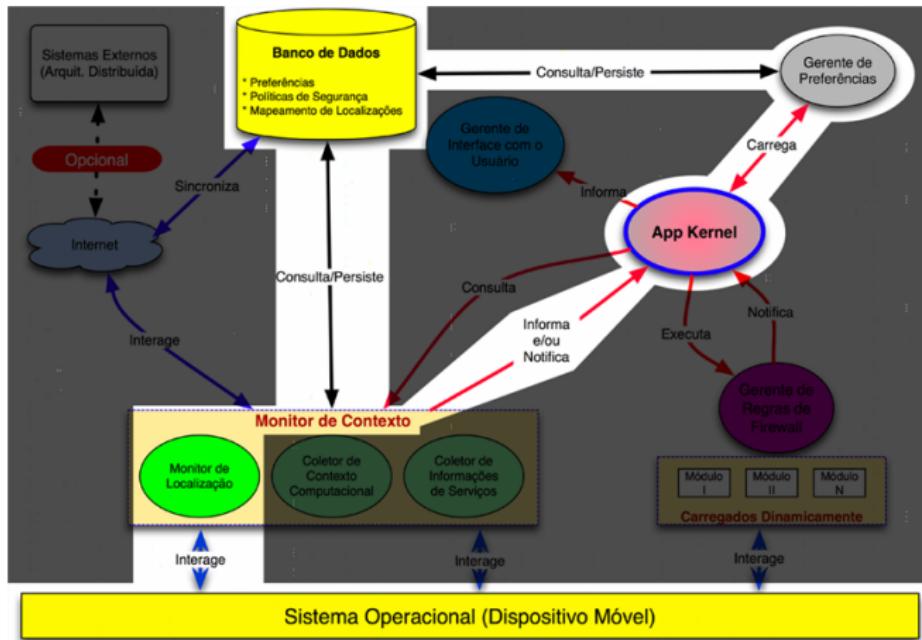
# Controlando Interfaces de Rede



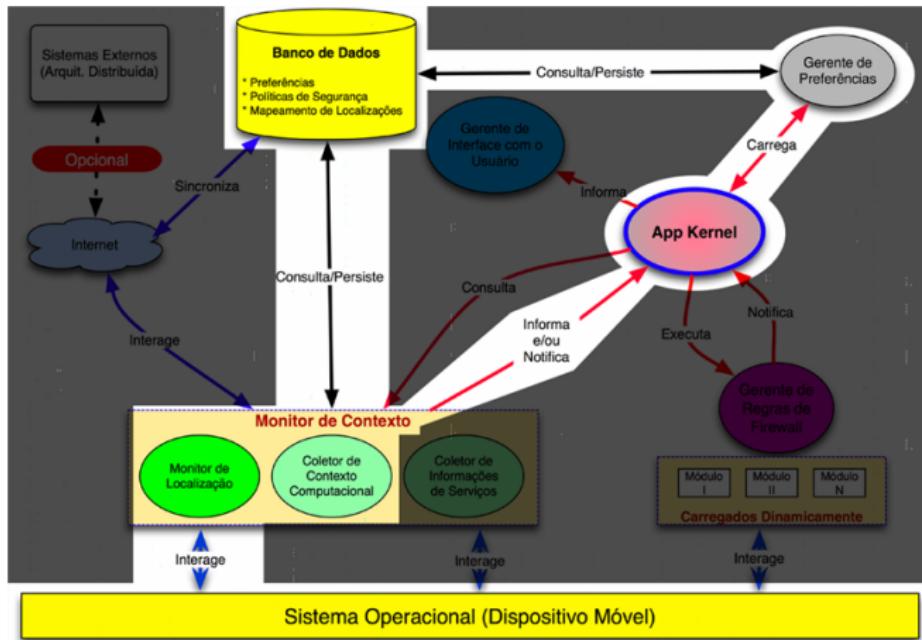
# Controlando Interfaces de Rede



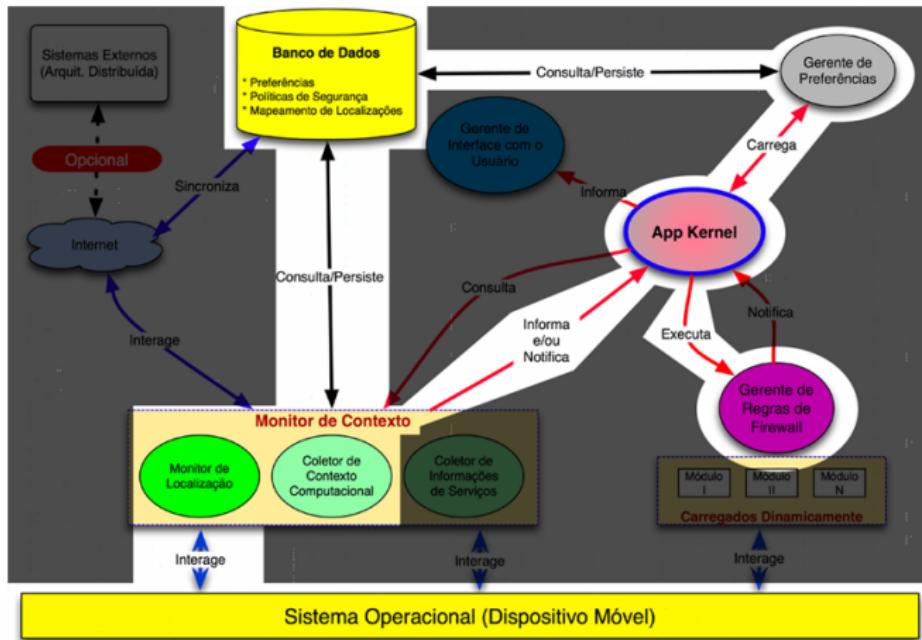
# Controlando Interfaces de Rede



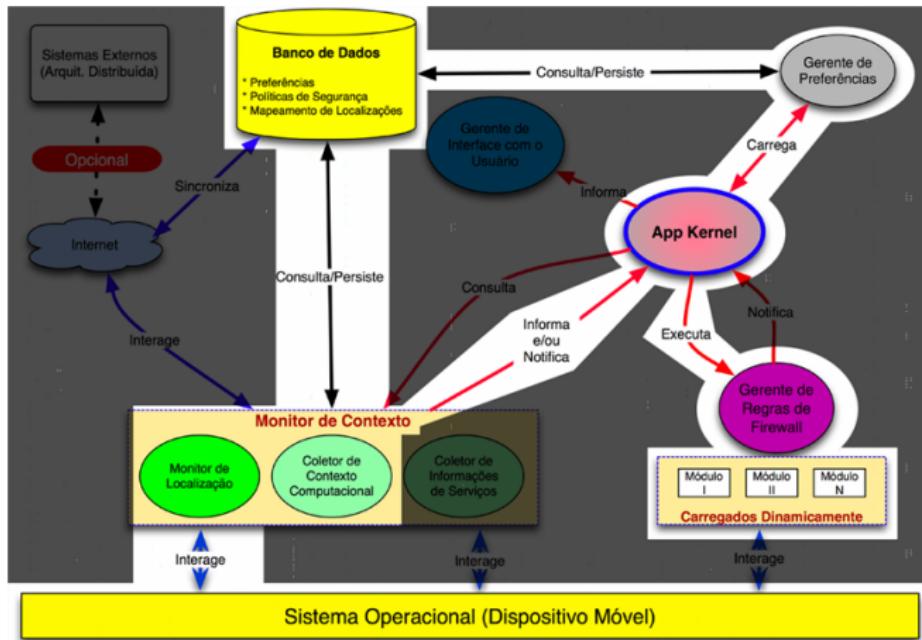
# Controlando Interfaces de Rede



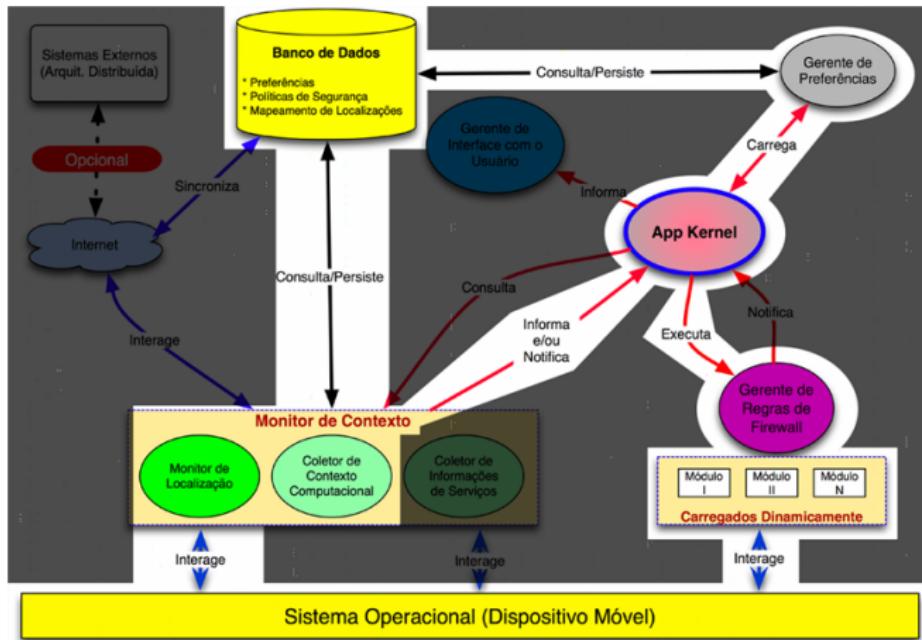
# Controlando Interfaces de Rede



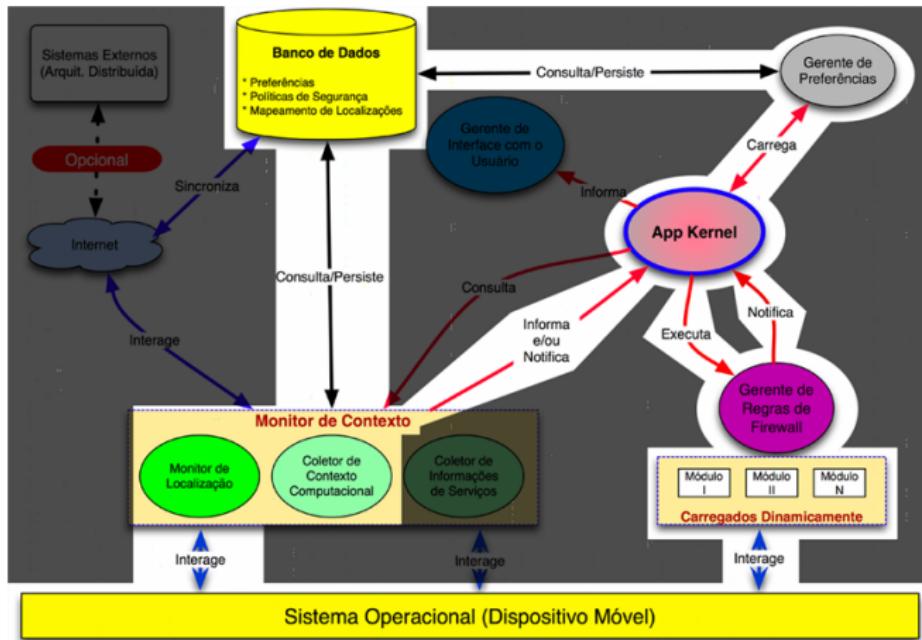
# Controlando Interfaces de Rede



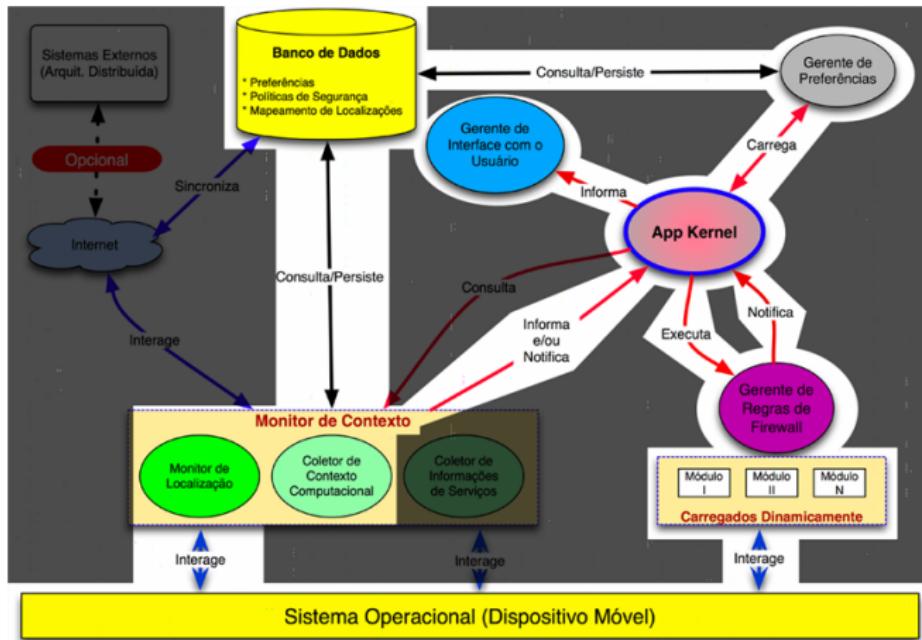
# Controlando Interfaces de Rede



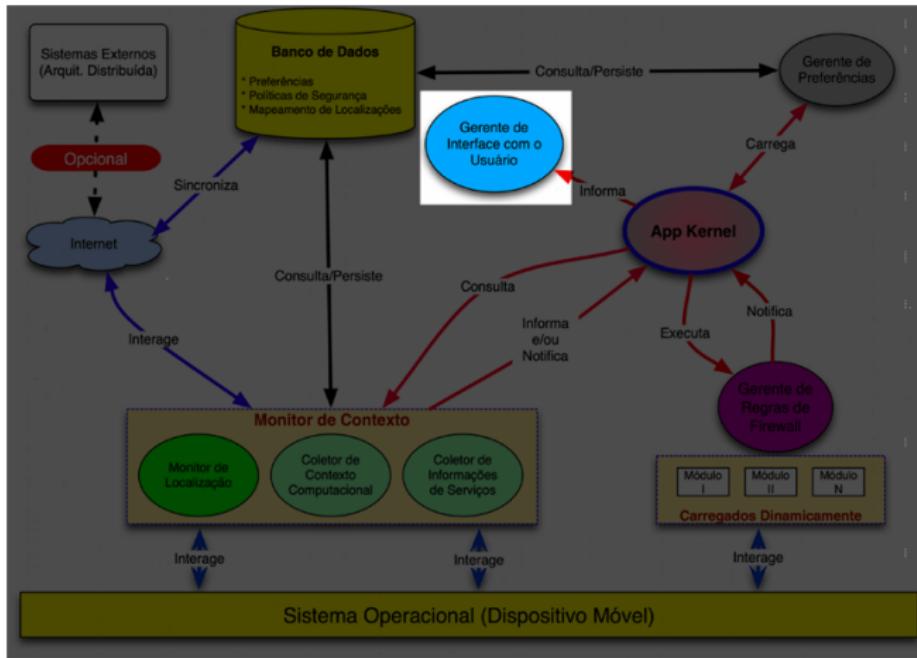
# Controlando Interfaces de Rede



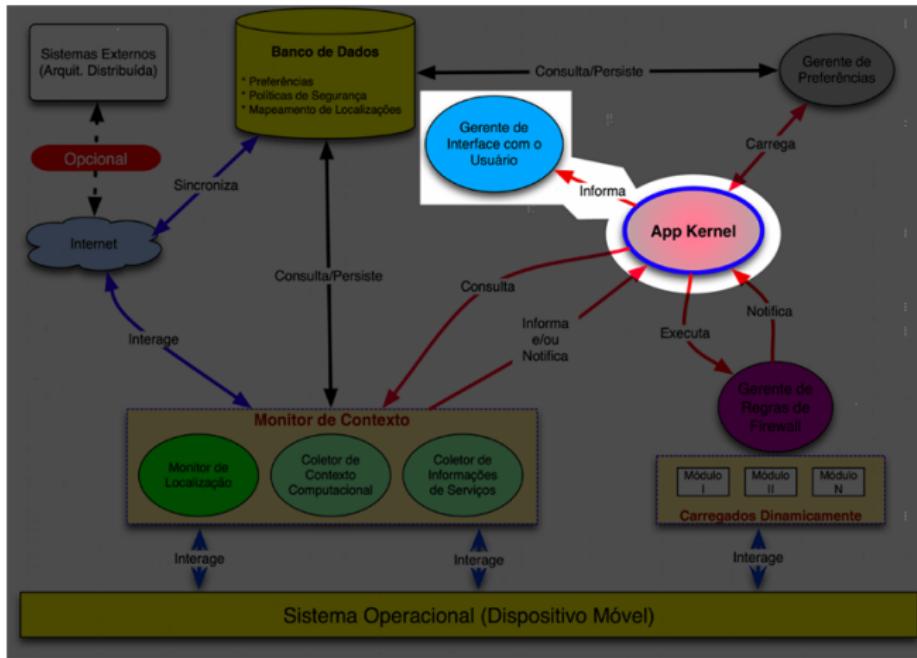
# Controlando Interfaces de Rede



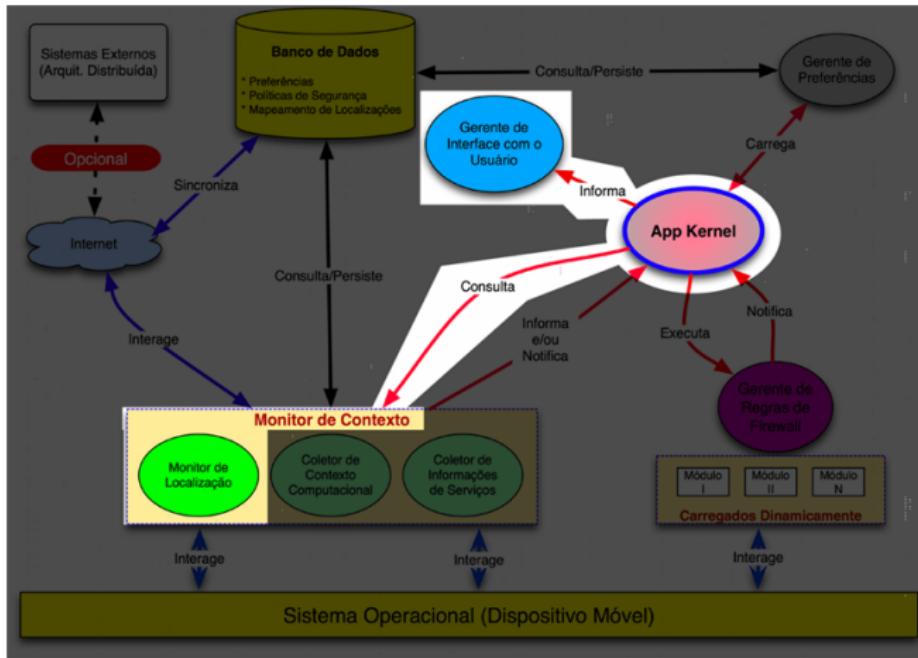
# Restringindo acessos



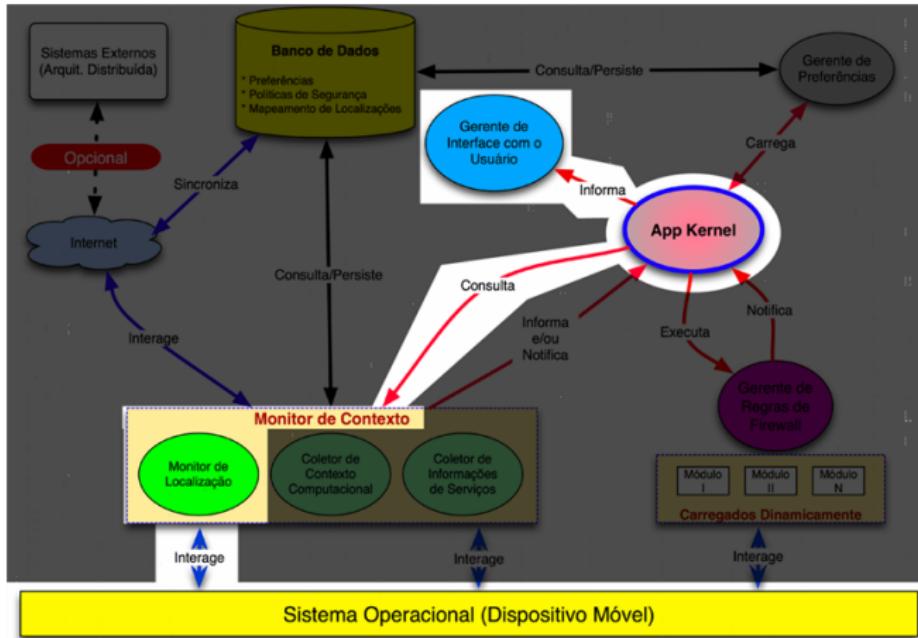
# Restringindo acessos



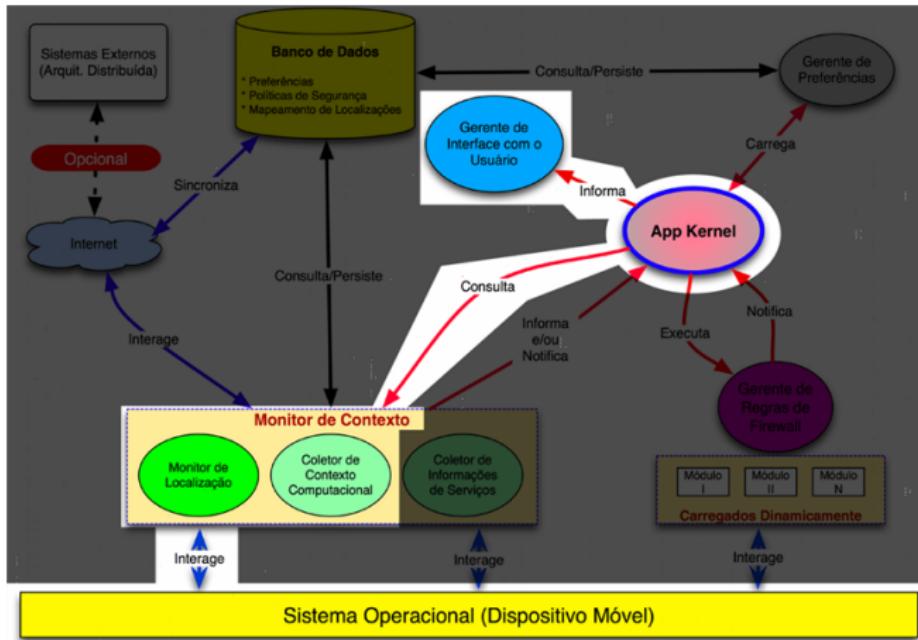
# Restringindo acessos



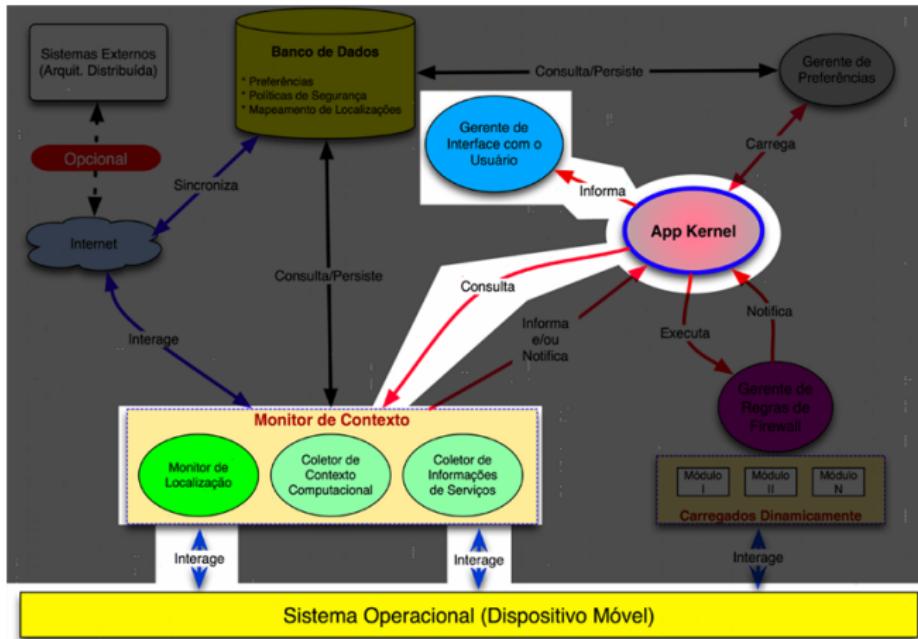
# Restringindo acessos



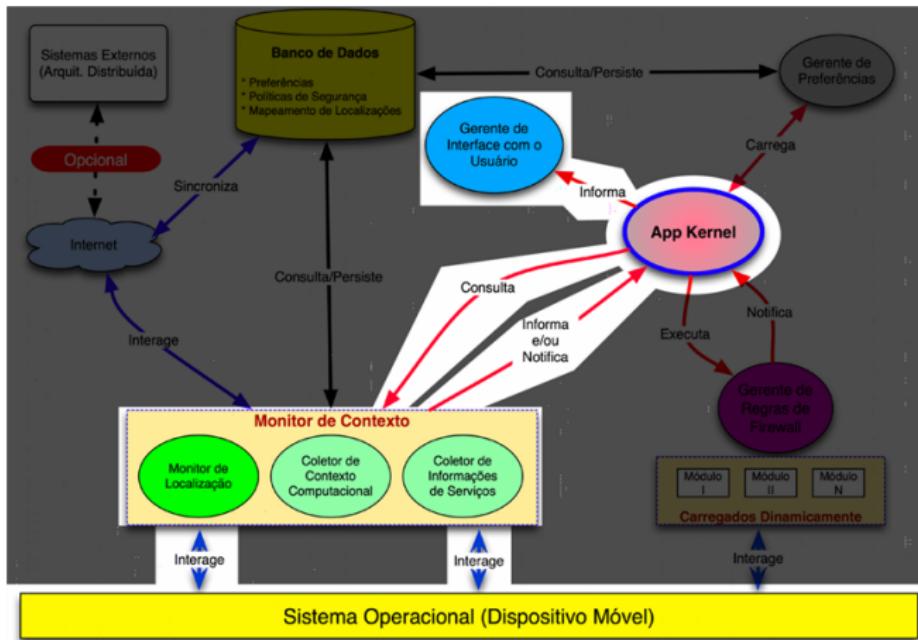
# Restringindo acessos



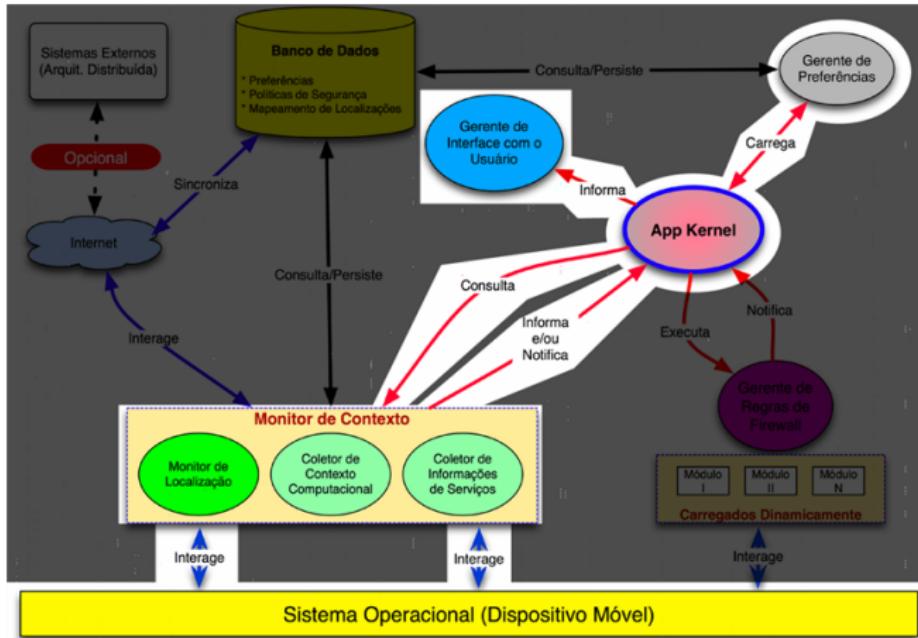
# Restringindo acessos



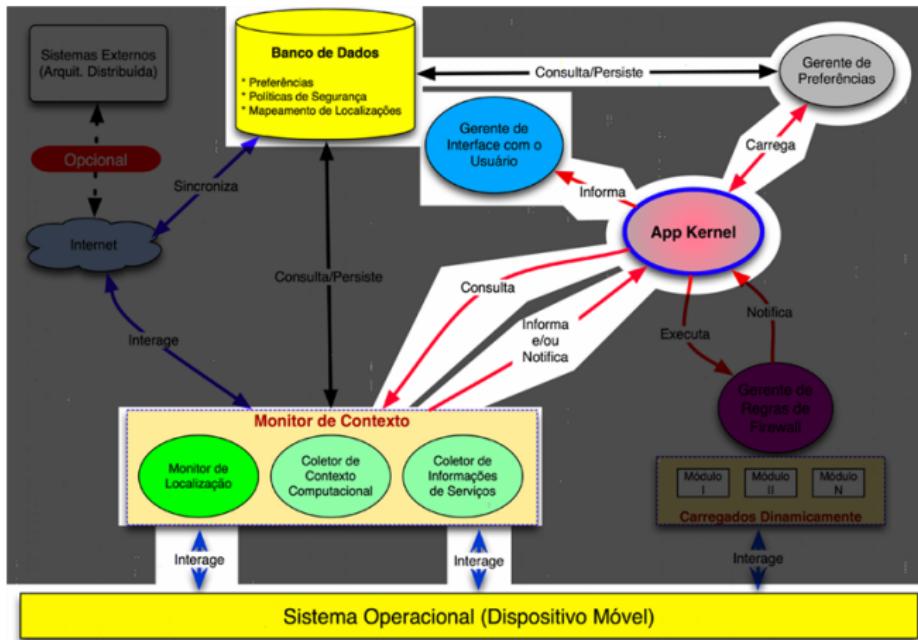
# Restringindo acessos



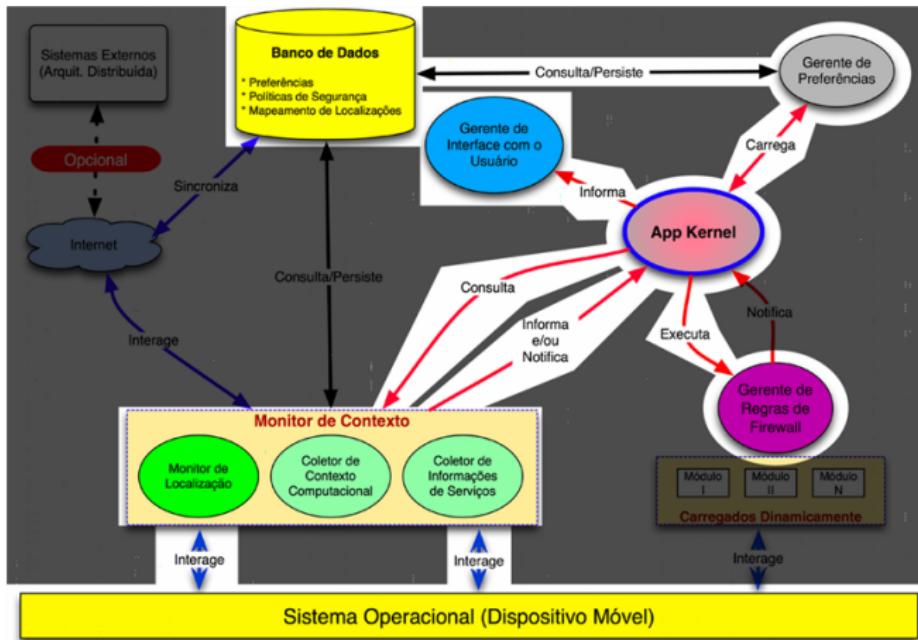
# Restringindo acessos



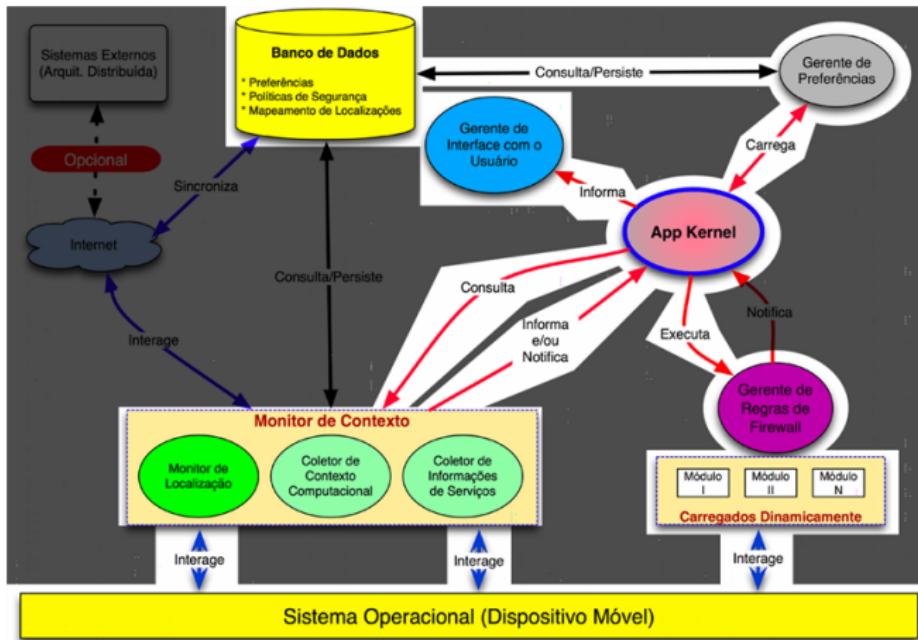
# Restringindo acessos



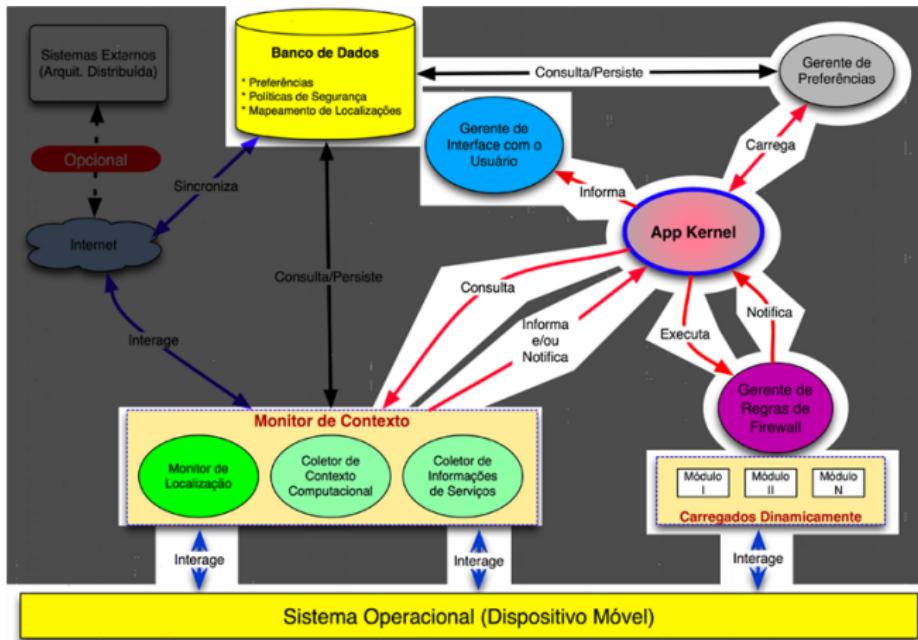
# Restringindo acessos



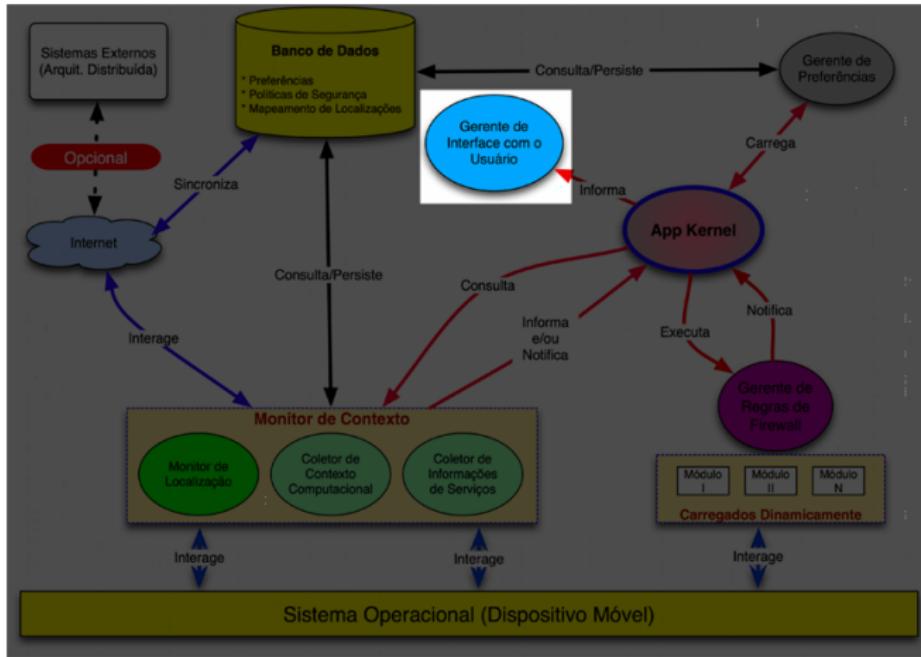
# Restringindo acessos



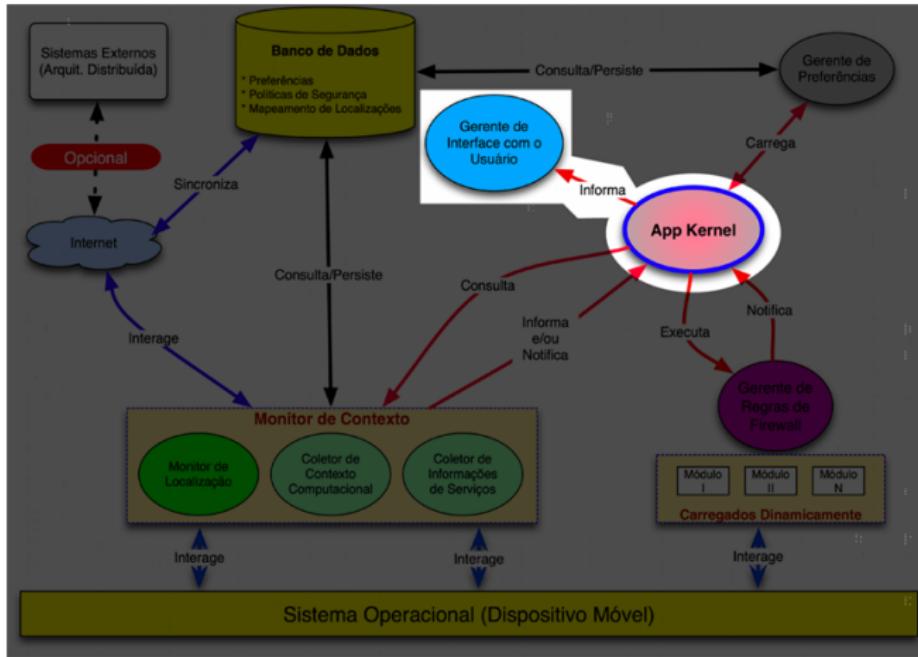
# Restringindo acessos



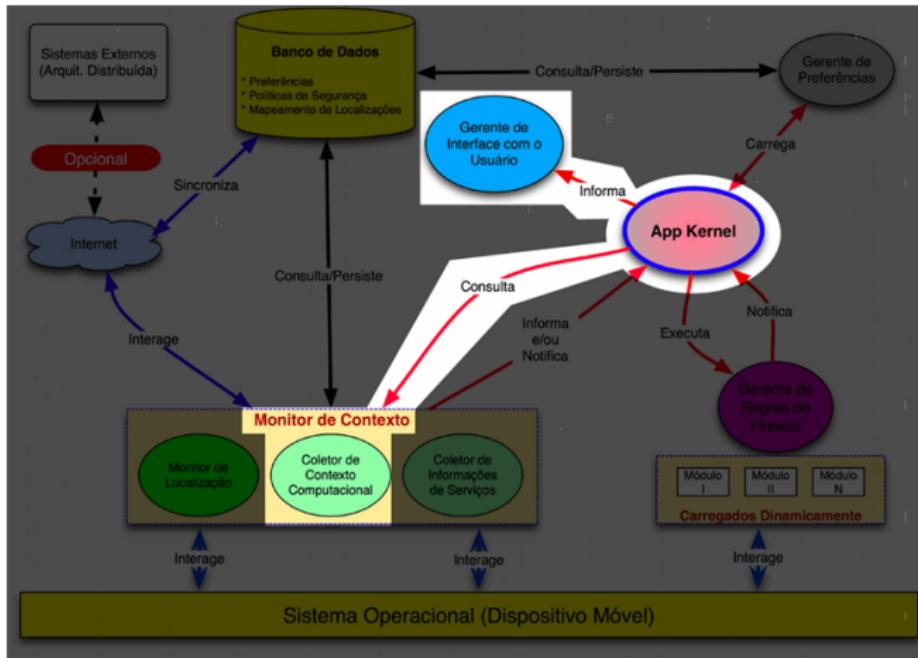
# Sincronização Manual do Banco de Dados



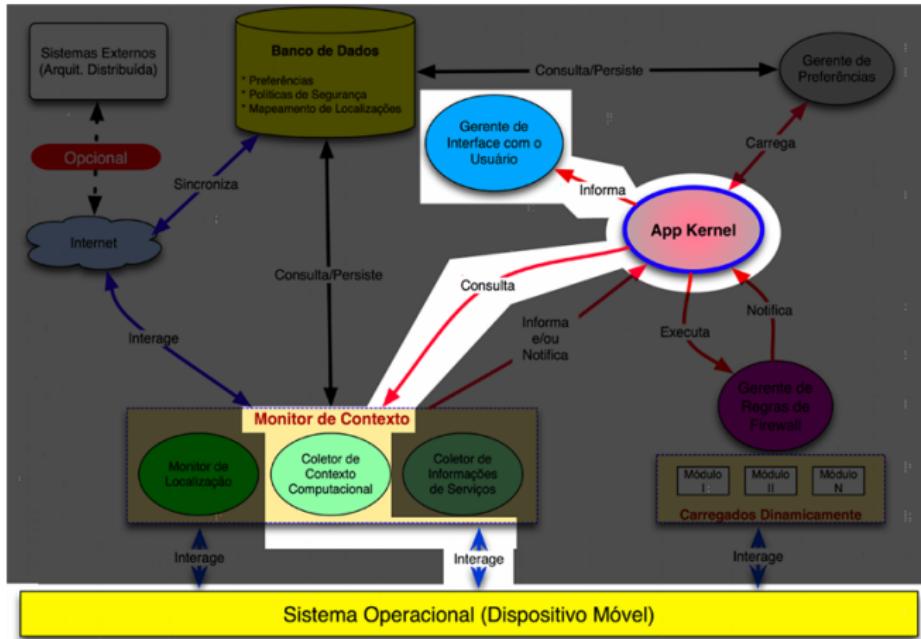
# Sincronização Manual do Banco de Dados



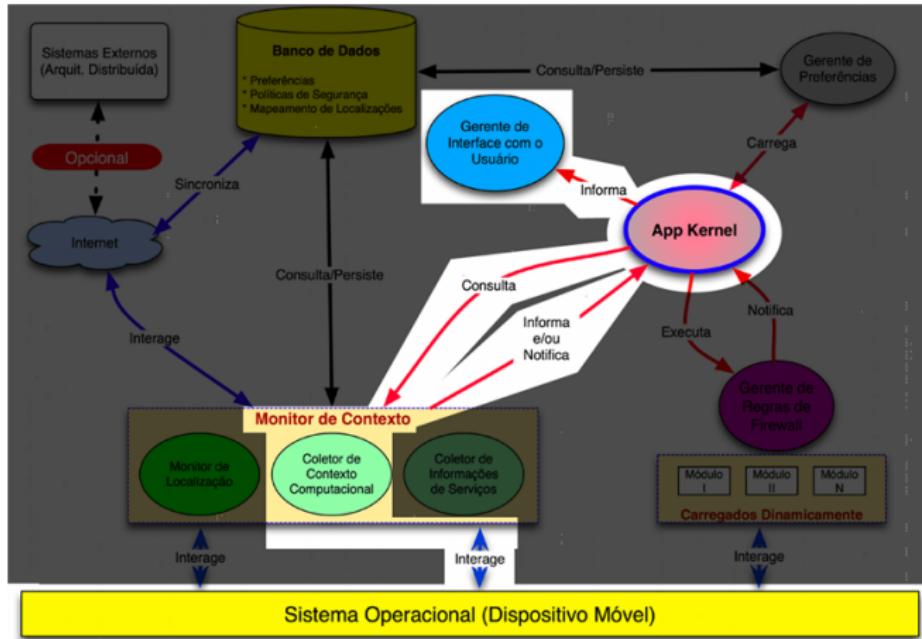
# Sincronização Manual do Banco de Dados



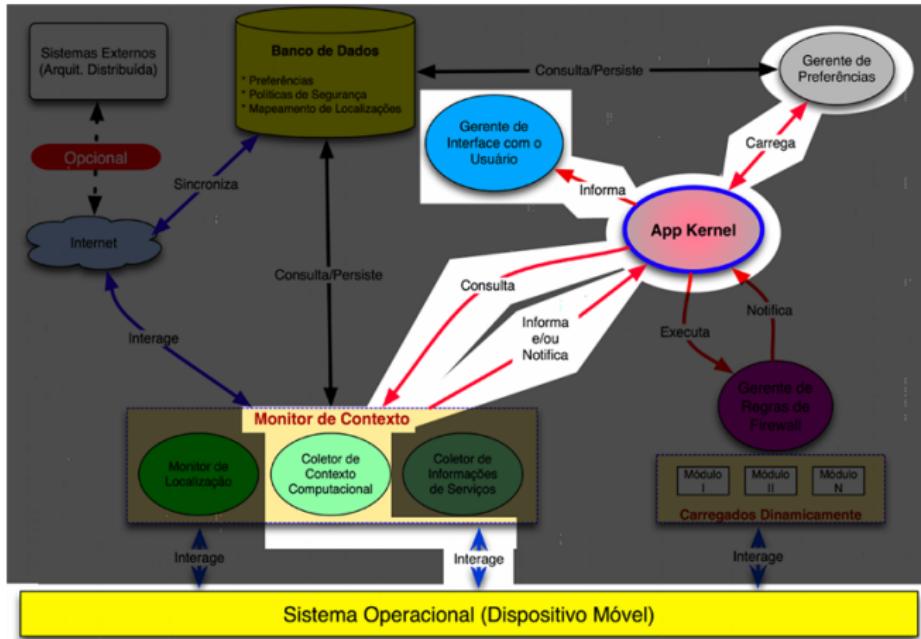
# Sincronização Manual do Banco de Dados



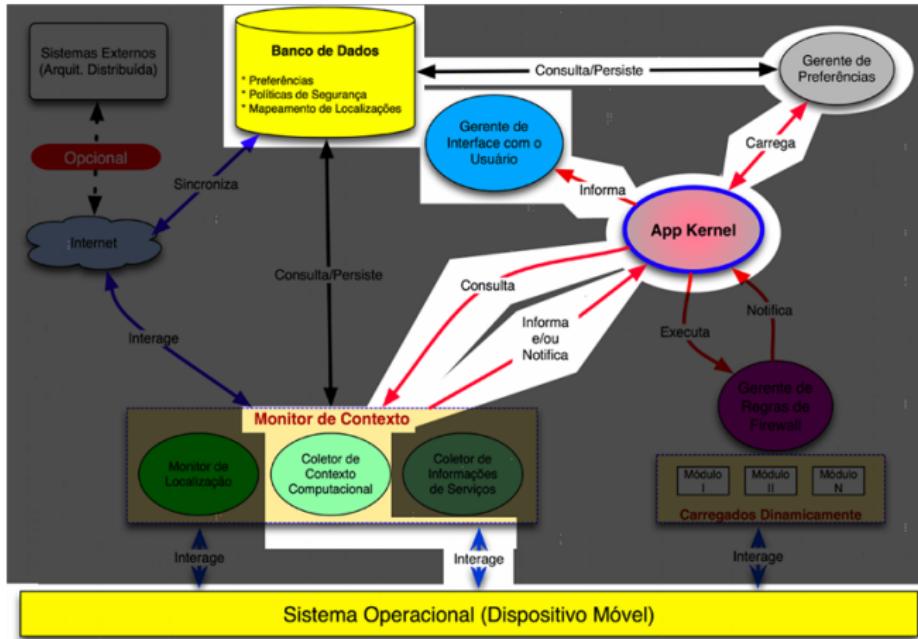
# Sincronização Manual do Banco de Dados



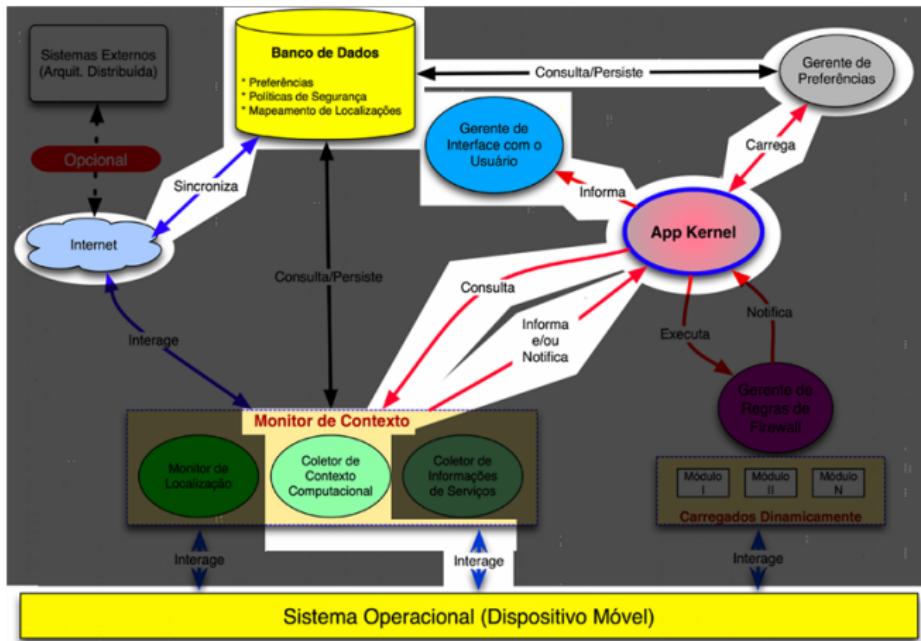
# Sincronização Manual do Banco de Dados



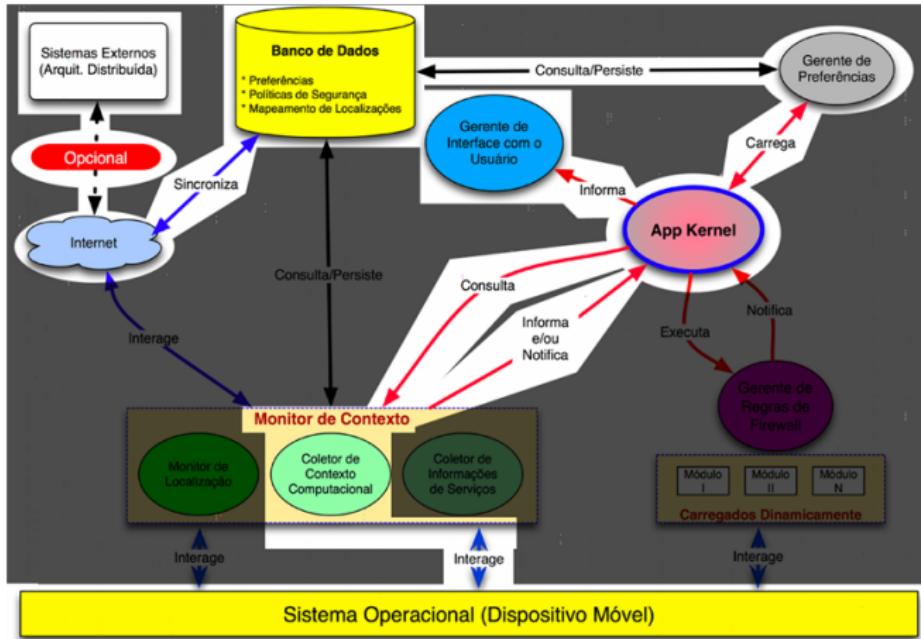
# Sincronização Manual do Banco de Dados



# Sincronização Manual do Banco de Dados



# Sincronização Manual do Banco de Dados



## Nossa Contribuição

Nossa principal contribuição é o **Projeto Arquitetural de um Firewall Pessoal para Dispositivos Móveis**, que se utiliza do paradigma de localização do usuário para carregar preferências e políticas de segurança.

# Nossa Contribuição I

- **[SEGURANÇA]**

Aumentar o nível de segurança contra os ataques vindo da rede de comunicação;

- **[CONTROLE]**

Controlar o acesso aos recursos do dispositivo móvel e as informações;

- **[POLÍTICAS E PREFERÊNCIAS]**

Flexibilidade para que o usuário execute, crie e edite suas preferências e políticas de segurança;

# Diferencial do Fênix Firewall System I

- **[LOCALIZAÇÃO]**

Carregamento de Políticas e Preferências baseado na localização do usuário;

- **[INTERATIVIDADE CONTROLADA]**

Nível de Interatividade controlada pelo usuário;

- **[META-POLÍTICAS]**

Meta-políticas exportáveis;

- **[NOTIFICAÇÃO]**

Serviço de notificação do usuário via Web;

# Trabalhos Futuros

- Implementar o recurso de **meta-políticas** para outras plataformas de hardware (Ex.: Desktop, Tablet, Servidores etc);
- Integrar diferentes serviços de localização à Arquitetura Distribuída (Ex.: RFID, Placelab, MoCA etc);
- Arquitetura distribuída para detecção de riscos e falhas de segurança (Ex.: CVE e CVSS);
- Arquitetura distribuída extensível para trabalhos futuros(Detectão de intrusão, Análise Inteligente etc);

# Leituras Recomendadas I

-  **W.R. Bellovin, S.M. and Cheswick**  
*Network firewalls.*  
IEEE Communications Magazine, Vol. 32
-  **FIRST (Forum of Incident Response and Security Teams)**  
*CVSS (Common Vulnerability Scoring System).*  
<http://www.first.org/cvss/>
-  **McAfee**  
*SAGE (Relatório Semestral de Segurança da McAfee).*  
2008.  
[http://www.mcafee.com/us/local\\_content/reports/sage\\_2008.pdf](http://www.mcafee.com/us/local_content/reports/sage_2008.pdf)

## Leituras Recomendadas II

 Instituto de Pesquisa IDC

*Brazil IT Investment Trends Insurance. 2007*

<http://www.idclatin.com/>

► GSM 03.40

*Technical realization of the Short Message Service (SMS)*

<http://www.3gpp.org/ftp/Specs/html-info/0340.htm>

► Durlacher Researchs Ltd

*Mobile Commerce Report*

[www.durlacher.com/research/res-reports.asp](http://www.durlacher.com/research/res-reports.asp)

## Leituras Recomendadas III

[7] Snort

*Open Source Network Intrusion Detector*

<http://www.snort.org/>

[8] Placelab

*A privacy-observant location system.*

<http://www.placelab.org/>

[9] Pontifícia Universidade do Rio De Janeiro

*MoCA (Mobile Collaboration Architecture)*

<http://www.lac.inf.puc-rio.br/moca/>

## Leituras Recomendadas IV

[10] iPhone

*The iPhone.* Apple Inc.,2008.

<http://en.wikipedia.org/wiki/IPhone>