

Autenticação baseada em 2 fatores

Nelson Murilo

Agenda

- Motivação
- Tipos de 2FA
- Ataques
- Soluções

Motivação

- **Vários bancos e sites estão usando autenticação com 2 fatores**
- **Vários usuários continuam tendo suas credenciais capturadas**
- **Por que?**

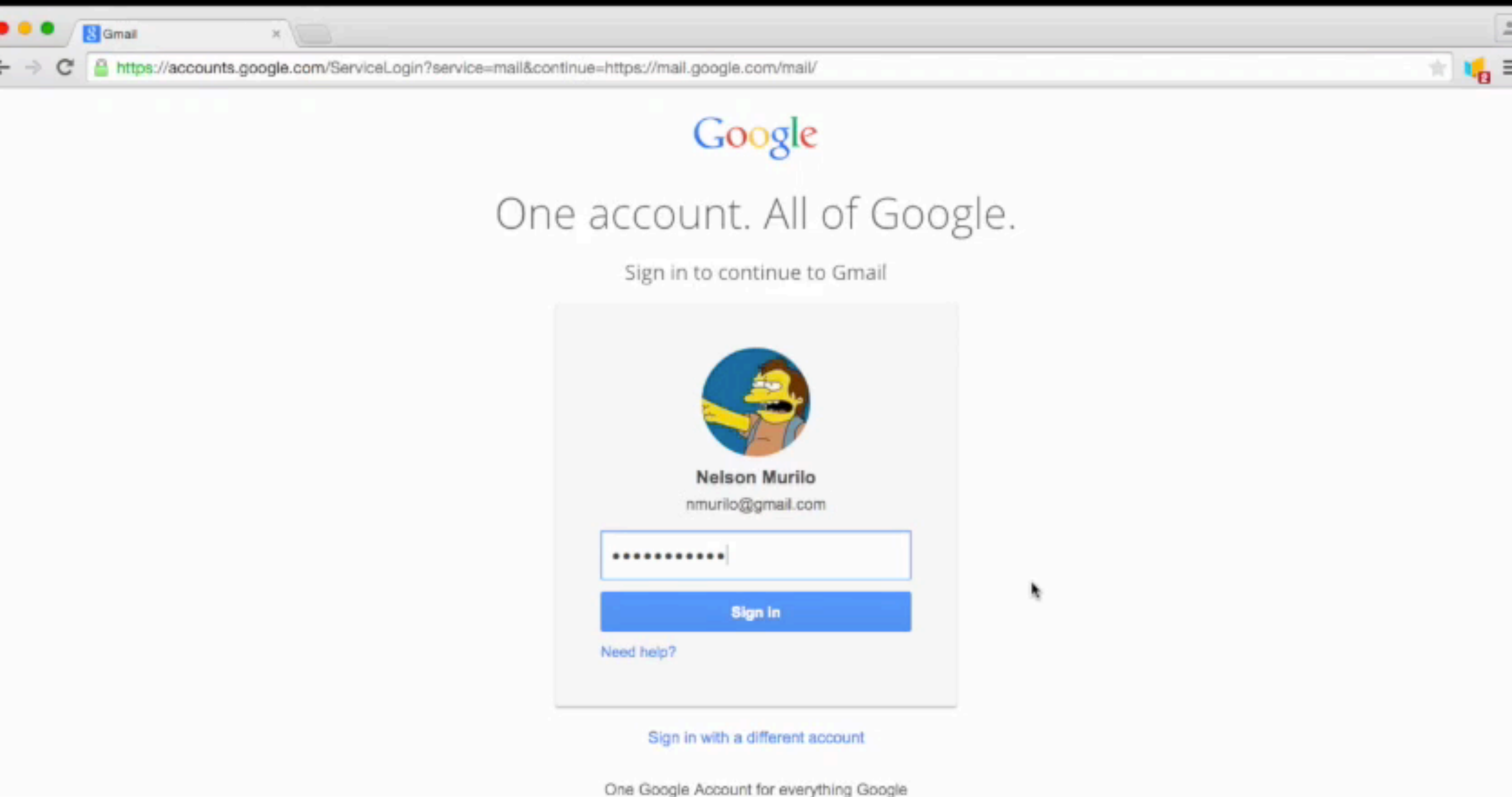
Fatores

- O que se sabe
- O que se tem
- O que se é

Tipos

- OTP   
- Internet + SMS (Reverso)
- Ligação Reversa
- Biometria

OTP



idgnow.com.br/internet/2015/04/21/adeus-senhas-paypal-quer-que-usuarios-tomem-comprimidos-de-acesso/

Internet

Adeus, senhas: PayPal quer que usuários tomem "comprimidos de acesso"

PC World / EUA


21 de abril de 2015 - 14h10

Segundo empresa de pagamentos, métodos externos como impressões digitais e escaneamento de íris são "antiquados".

70

 Tweet

34

 Share


45

 Share

5

 +1

 Imprima

 Mais +



Microsoft Azure



Falamos Hadoop

Java, Hive, Pig, LINQ, .NET
No Azure, o Hadoop fala

Teste grátis 

ÚLTIMAS NOTÍCIAS



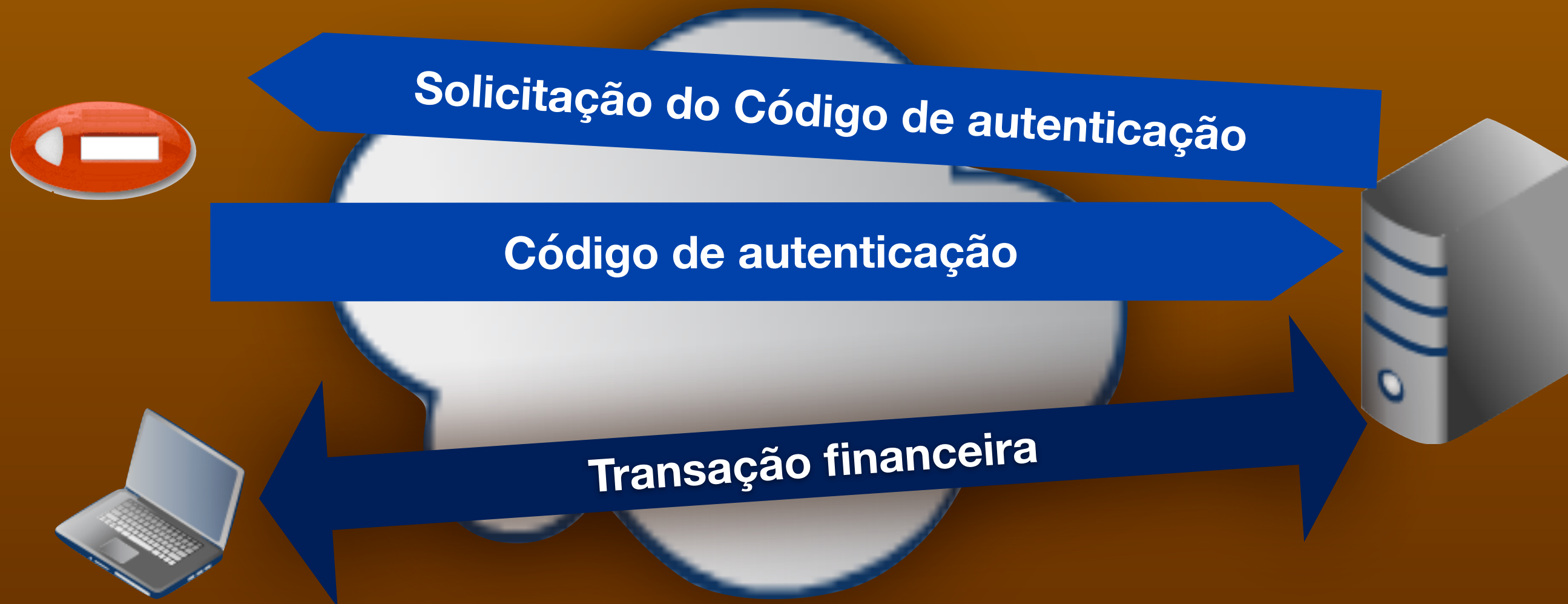
Justiça arquiva
e libera uso do

Revogada liminar que proib
Uber

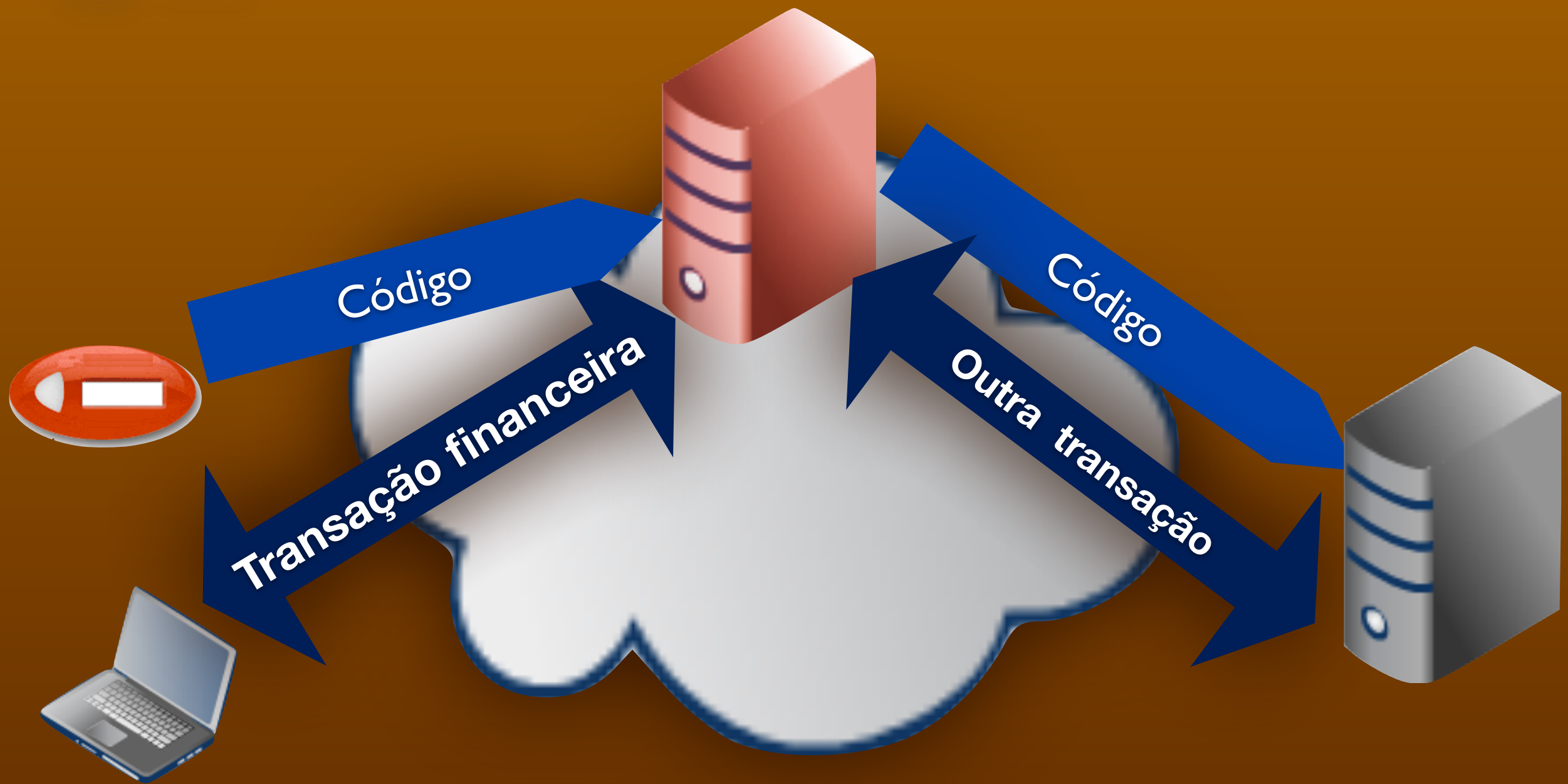


Pesquisa do Li

OTP

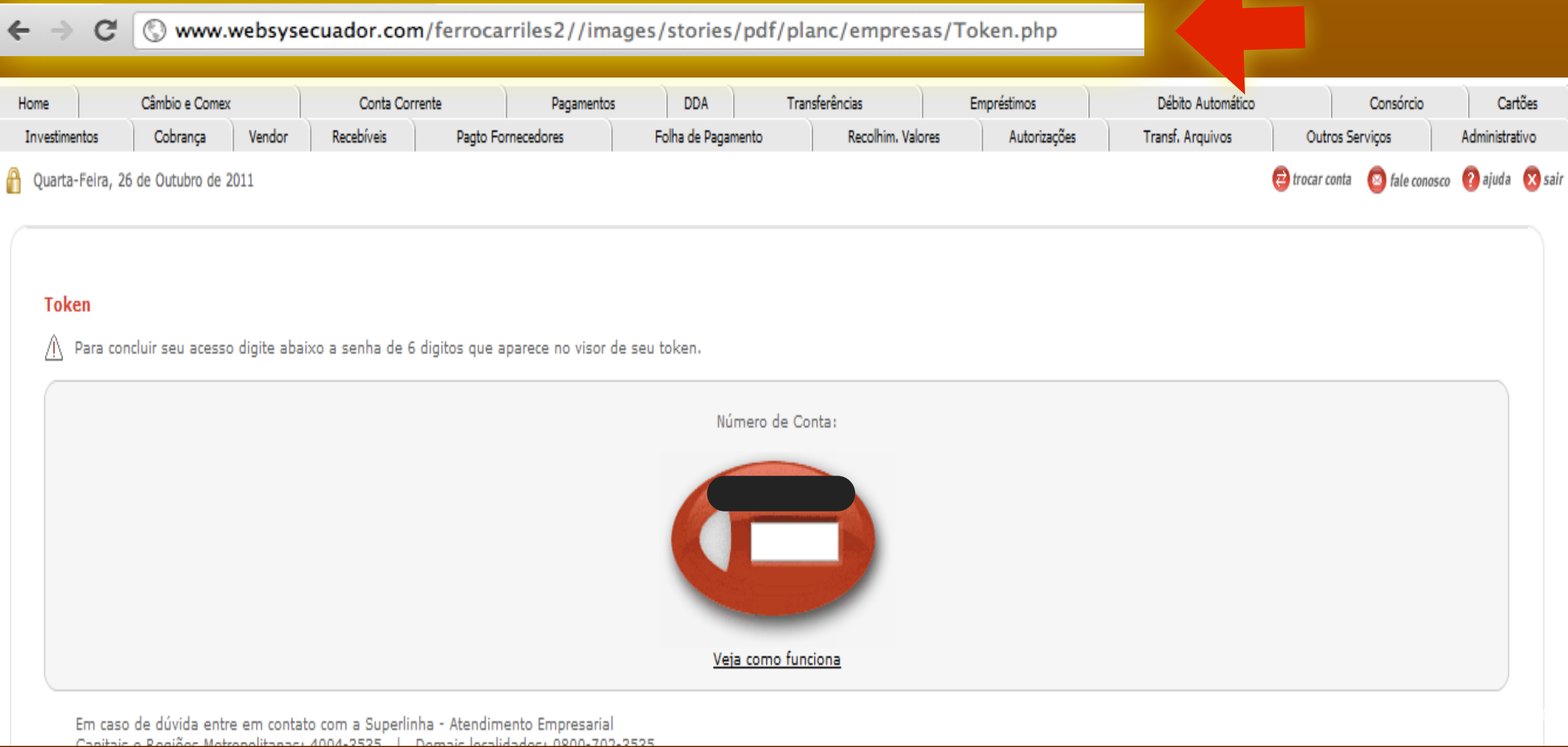


OTP



Man in the middle attack

Internet + Hard Token




The screenshot shows a web browser window with the address bar displaying `www.websysecuador.com/ferrocarriles2//images/stories/pdf/planc/empresas/Token.php`. A large red arrow points from the title 'Internet + Hard Token' to the address bar. The page has a navigation menu with various options like 'Home', 'Câmbio e Comex', 'Conta Corrente', etc. The main content area is titled 'Token' and contains a warning icon and text: 'Para concluir seu acesso digite abaixo a senha de 6 digitos que aparece no visor de seu token.' Below this is a large red oval representing a token, with a black bar obscuring the top part and a white box for the bottom part. The text 'Número de Conta:' is above the token, and 'Veja como funciona' is below it. At the bottom, there is contact information for 'Superlinha - Atendimento Empresarial'.

Token

⚠ Para concluir seu acesso digite abaixo a senha de 6 digitos que aparece no visor de seu token.

Número de Conta:



[Veja como funciona](#)

Em caso de dúvida entre em contato com a Superlinha - Atendimento Empresarial
Capitais e Regiões Metropolitanas: 4004-2525 - Demais localidades: 0800-702-2525

Man in the middle attack

invoeren rekening- en pasnummer

Neem het rekeningnummer en pasnummer over van uw pas.

rekeningnummer

pasnummer

Telefoonnummer

☐ Onthoud mijn rekeningnummer en pasnummer.



op uw e.dentifier2

- Controleer of uw pas is ingevoerd
- Druk op **1** Inloggen
- Toets uw pincode in
- Druk op **OK**
- Een response wordt getoond



invoeren response

Vul de response in

Klik op OK onder in het scherm.

OTP

Man in the middle attack

- Manual ou Robô
- Janela de ataque ~2 minutos
- Troca da transação legítima pela do fraudador

OTP

- Desvinculado da transação
- Man in the middle
- Man in the browser

Internet + SMS (reverso)

Uso:

- Identificação de computador
- Autenticação
- Confirmação de transação

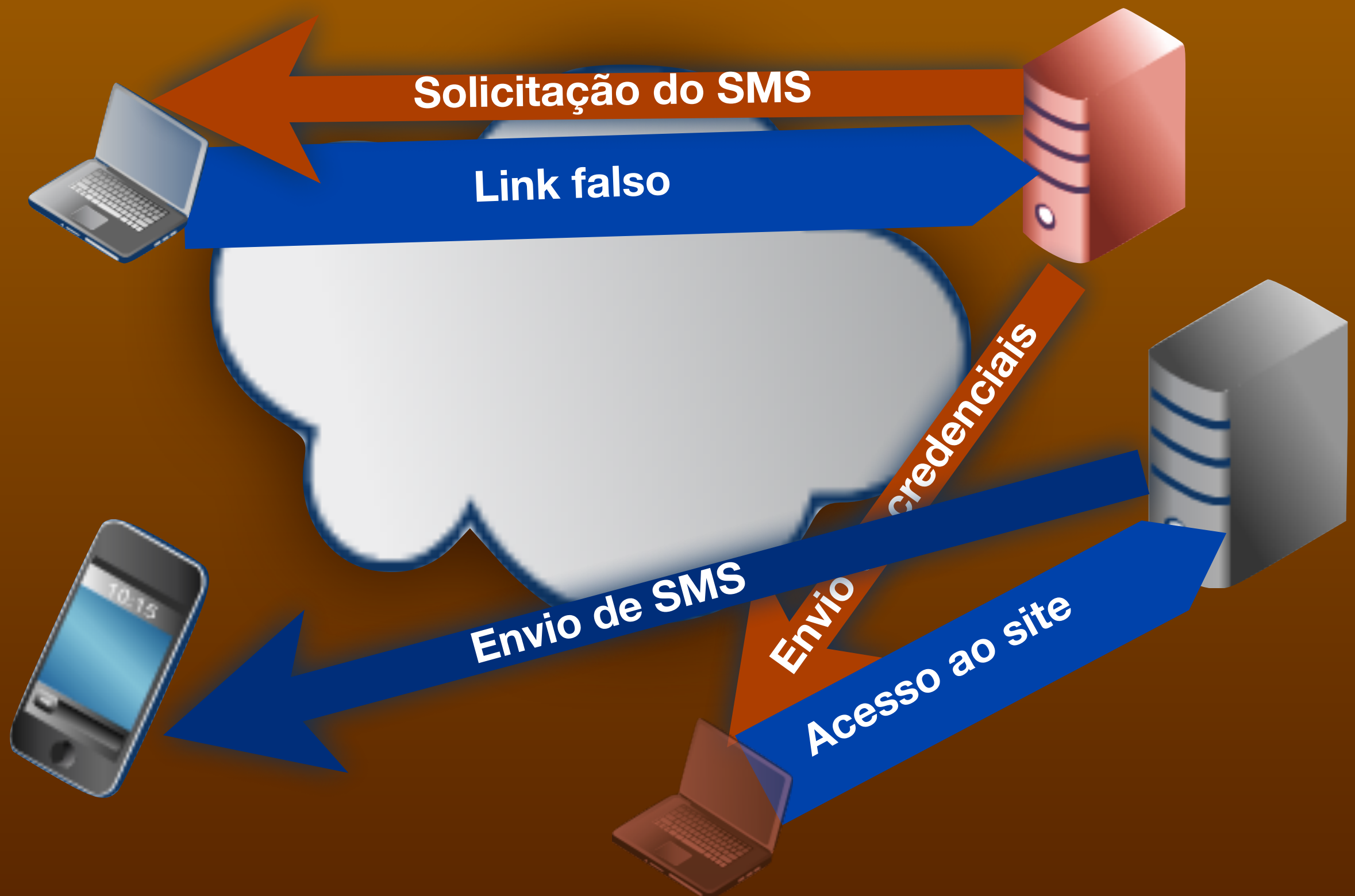
Internet + SMS

- Man in the Middle
- Man in the Browser
- Man in the Mobile

Internet + Celular



Internet + Celular



Internet + Celular

ação de Segurança

ento e

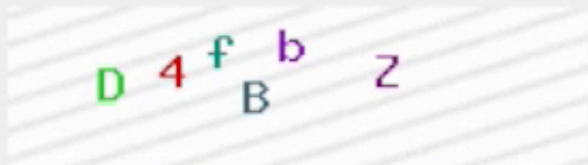
urança

as conc

or favor

Iniciando a Instalação de Segurança Obrigatória

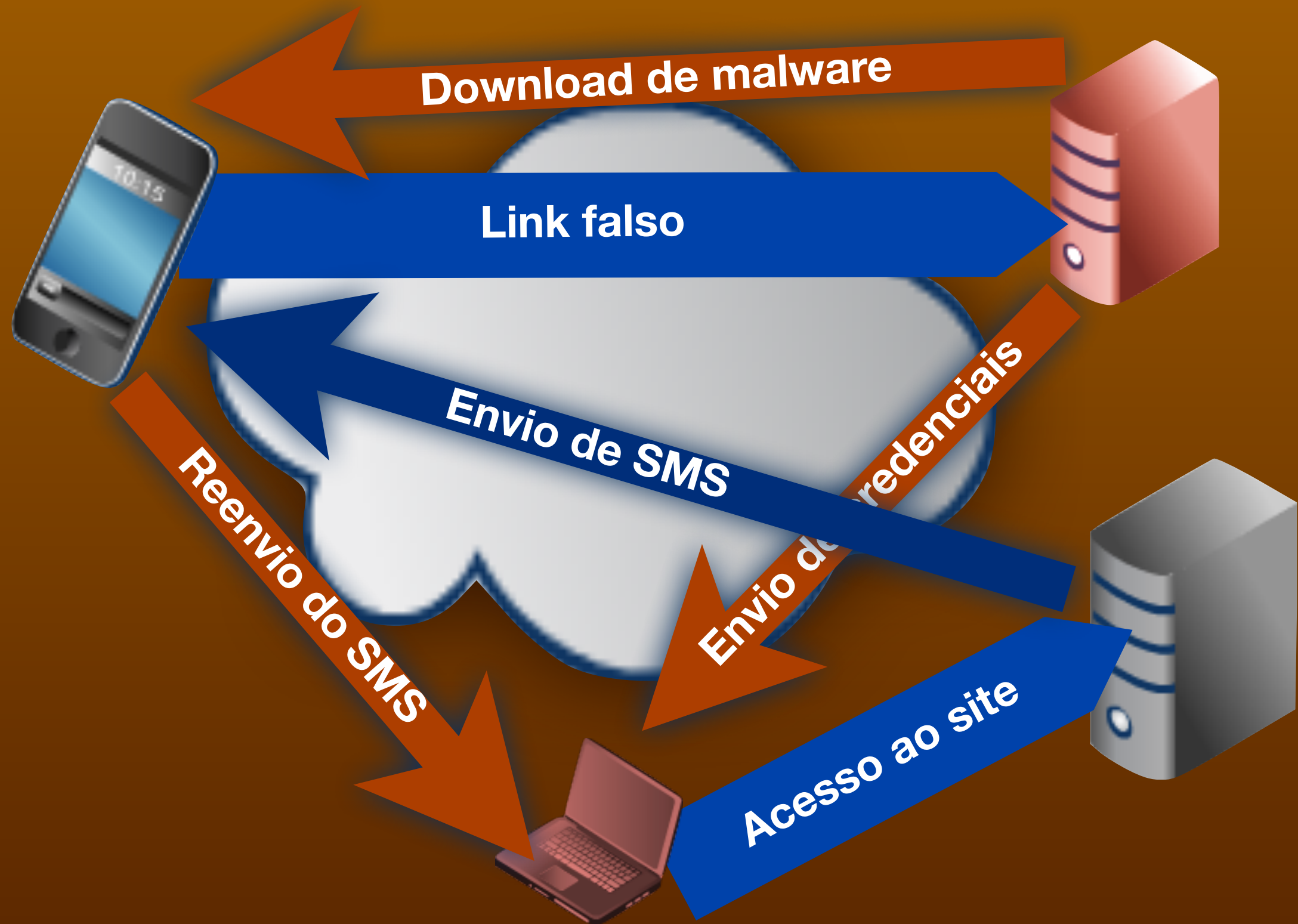
Digite o que você vê dentro da imagem!



es no acesso ao

overno): 3003-0500 (capitais e regiões que dispõem do serviço 3003), 0800-729-0500 (demais localidades)

Internet + Celular



Internet + Celular

Man in the middle attack



On-line ou Robô



Janela de ataque ~1 dia



Acesso com as credenciais
do usuário

OTP



2-Step Verification

You normally use a Security Key, but must use a verification code for this sign-in.



Enter the verification code generated by your mobile application.

Verify



Don't ask for codes again on this computer

[Problems with your code?](#)



OTP

2-Step Verification

Verification codes

App-specific
passwords

**Registered
computers**

Security Keys

2-Step Verification is: **ON**

Protecting your account since Jul

THIS COMPUTER

Turn off



This computer is not registered

When you sign in to your Google Account on this computer, you need to provide a verification code in addition to your password. You can change this during sign-in where you can tell us not to ask for a code again on this computer. We'll still ask for codes on other computers.

Register this computer

Internet + Celular

Man in the middle attack



On-line ou Robô



Janela de ataque ~1 dia




Acesso com as credenciais
do usuário

Internet + Celular

Ataque 3



Usuário acessa site falso e informa suas credencias



Em seguida o site falso informa que ele deve “sincronizar” o celular e instala malware



Atacante agora controla PC e celular

Internet + Ligação p/ usuário

Microfone



Ligação Reversa

- Gravador (captura de credenciais)
- Redirecionamento de chamada

Man in the Browser

Credenciais

Transação A

Transação B



Credenciais

Transação A

Método de
autenticação

Transação B



Redirecionamento de chamada

PROBLEMAS COM O TERMINAL
LIGUE SOMENTE PARA
O SAC

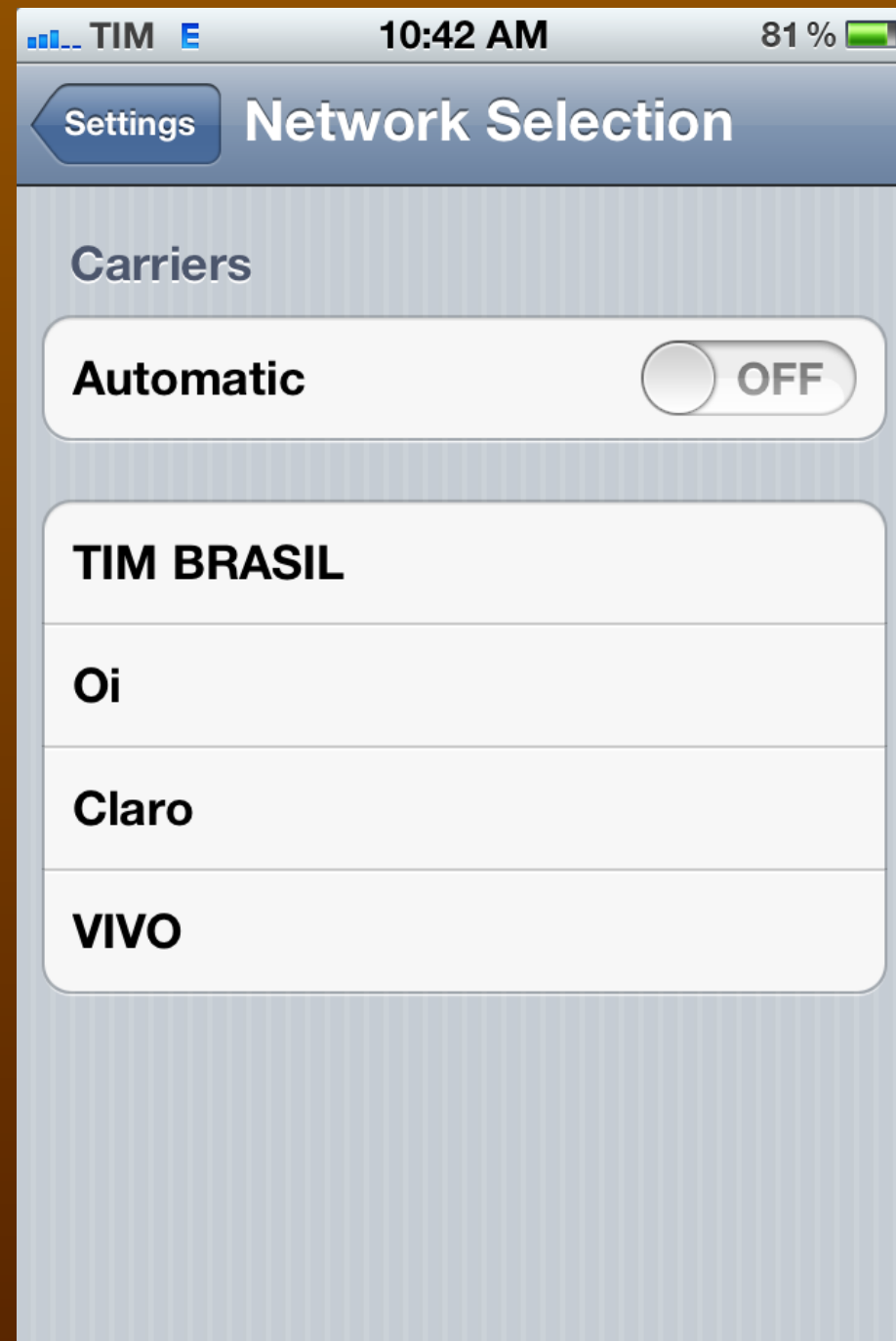
SAC

0800 8922 100

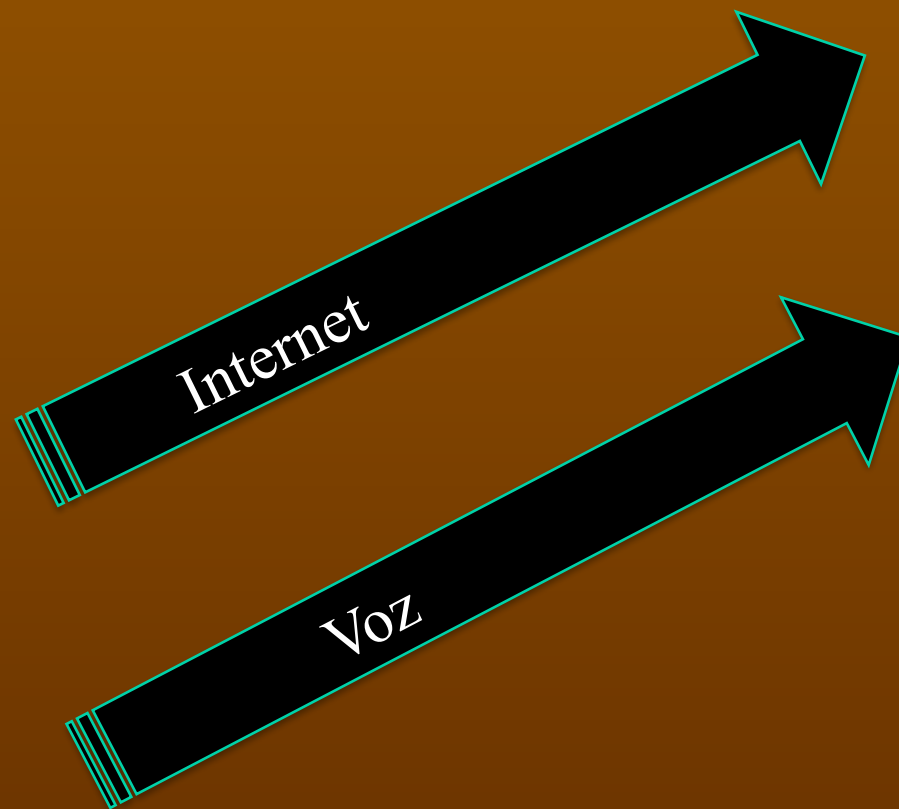
OU

4003 5619

Redirecionamento de chamada



Redirecionamento de chamada



Redirecionamento de chamada

The image shows a screenshot of the Asterisk Wiki page for OpenBTS, overlaid with the Asterisk logo. The page is titled "Welcome to OpenBTS" and provides information about the OpenBTS project, including a "Quick Links" section and a "What is OpenBTS?" section. The Asterisk logo is prominently displayed in the center, and the word "Asterisk" is written in large, stylized letters across the bottom.

Welcome to OpenBTS

This Trac is the home of the OpenBTS project.

To edit this wiki, you can login as user [personal](#) account from Kurtis (log in to edit)

BY-SA 3.0.

Quick Links:

- [OpenBTS developer community](#)

What is OpenBTS?

OpenBTS is a Unix application that uses a software radio interface to connect to a GSM air interface. It might even say that OpenBTS is a simplified form of [IMS](#) and VoIP backhaul forms the basis of a new type of cellular network that can be used for a variety of applications including rural cellular deployments and private cellular networks in remote areas.

Asterisk

• Power Supply

Table of Contents

- [What is OpenBTS?](#)
- [How do I get started?](#)
- [Where can I get the latest code?](#)
- [How do I build and install and run the code?](#)
- [Where documentation?](#)
- [How do I get support?](#)
- [Who else is using OpenBTS?](#)
- [Decoding UMTS](#)
- [SMQ2](#)

Navigation: [Home](#) » [Product Categories](#) » [USRP](#) » [rangepublic](#)

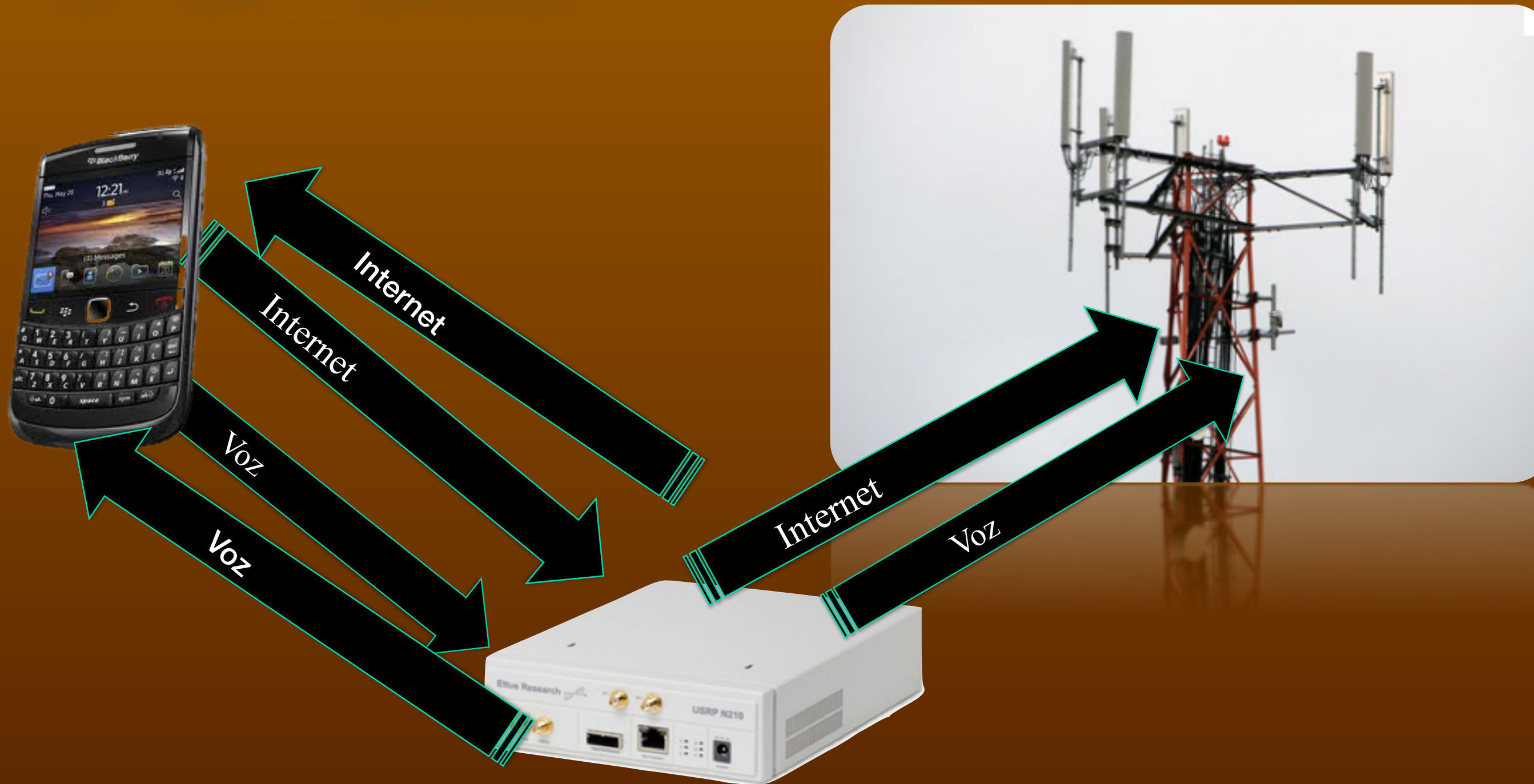
Search: [Search](#)

Links: [Login](#) | [Preferences](#) | [Help/Guide](#) | [About Trac](#) | [Roadmap](#) | [Browse Source](#) | [View Tickets](#) | [Search](#) | [Start Page](#) | [Index](#) | [History](#) | [Last Change](#)

Redirecionamento de chamada



Redirecionamento de chamada



Redirecionamento de chamada

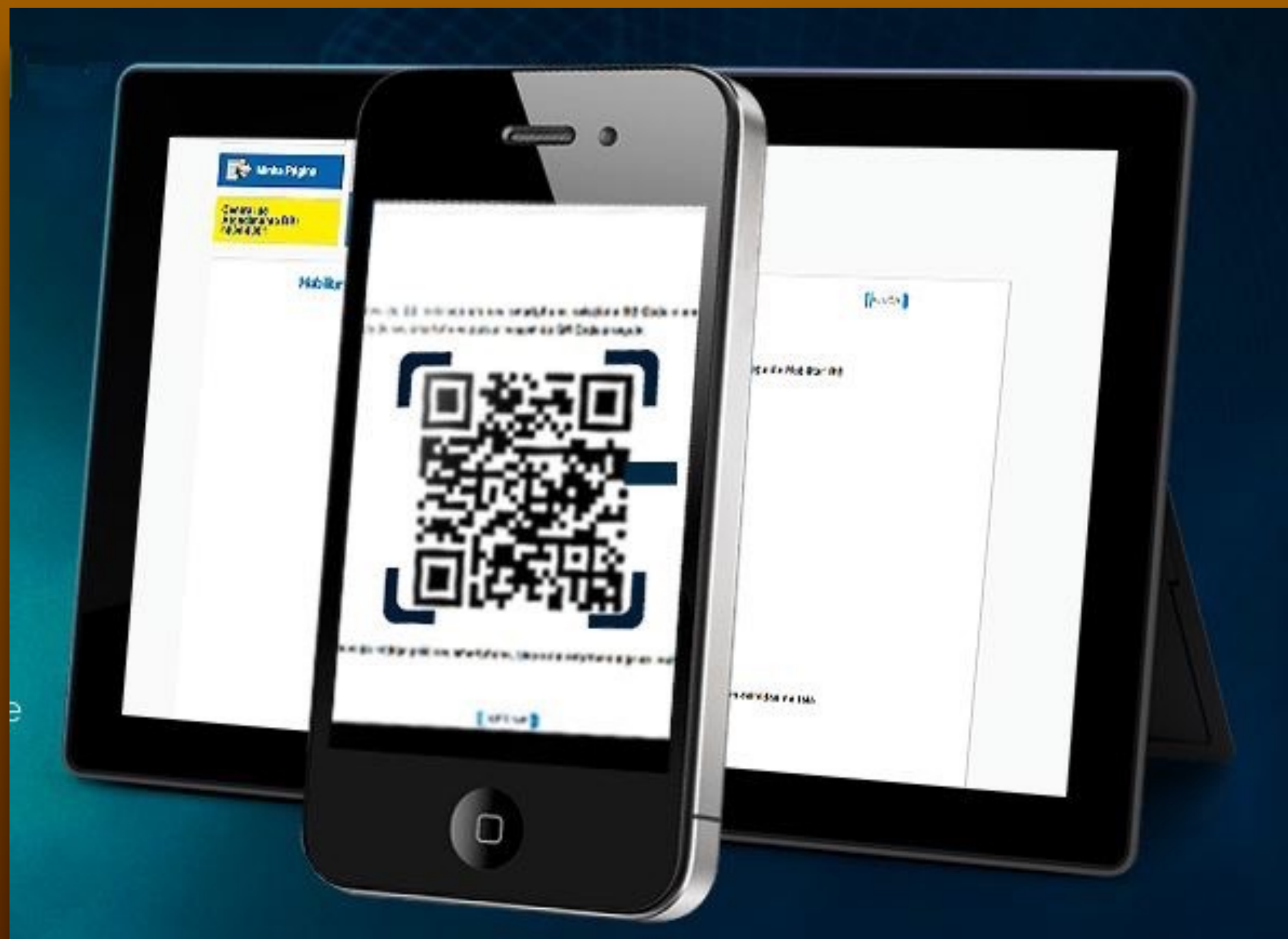


Redireccionamiento de llamada



Redireccionamiento de llamada







TRANSFERENCIA
CORRENTE P/ CO

DATA DA TRANS
HORA DA TRANS

VALOR TOTAL: 1

***** TRANSFER
CLIENTE: PEDRO
AGENCIA: 7988-2
170.159-2

Cancelar



Código Autorizador

008062

Confirmar

Confirmar



Autorizar

Recada

Voltar

Posicione o
em destaque
da câm

Volta

Autenticação baseada em 2 fatores

Nelson Murilo