

# GT-CIRD

## Caracterização e Identificação Remota de Dispositivos

João Paulo de Souza Medeiros

Universidade Federal do Rio Grande do Norte

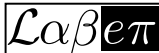
**19<sup>o</sup> WRNP**  
Workshop RNP  
7 | 8 MAIO  
Campos do Jordão | SP



# GT-CIRD: Caracterização e Identificação Remota de Dispositivos

WRNP 2018 – Programa de Internet Avançada

João Paulo de Souza Medeiros (DCT/UFRN, coordenador)  
Agostinho de Medeiros Brito Júnior (DCA/UFRN, coordenador adjunto)  
Antonio Alfredo Ferreira Loureiro (DCC/UFMG, coordenador adjunto)  
Rommel Wladimir de Lima (DI/UERN, coordenador adjunto)

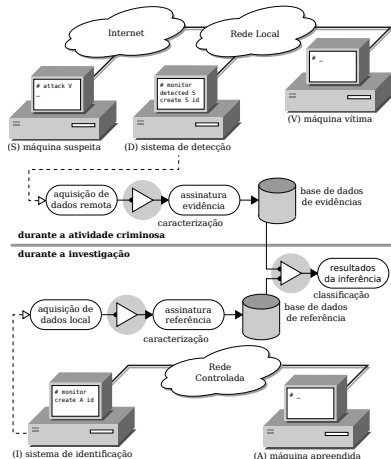


Laboratório de Elementos do Processamento da Informação – LabEPI  
Departamento de Computação e Tecnologia – DCT  
Universidade Federal do Rio Grande do Norte – UFRN

07 de maio de 2018

## GT-CIRD

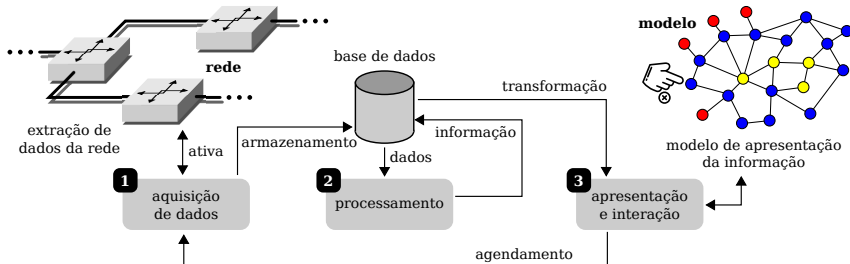
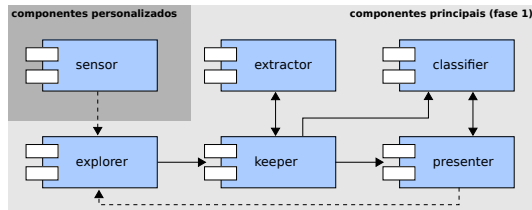
- ▶ **Objetivo:** criação de assinaturas para caracterização e identificação de máquinas remotas.
- ▶ **Caracterização:** busca por características que possam ser utilizadas para representar de forma eficaz algum componente de uma máquina remota.
- ▶ **Identificação:** utilização de métricas e métodos de comparação de assinaturas com o objetivo de classificar máquinas remotas.



# Arquitetura do Protótipo

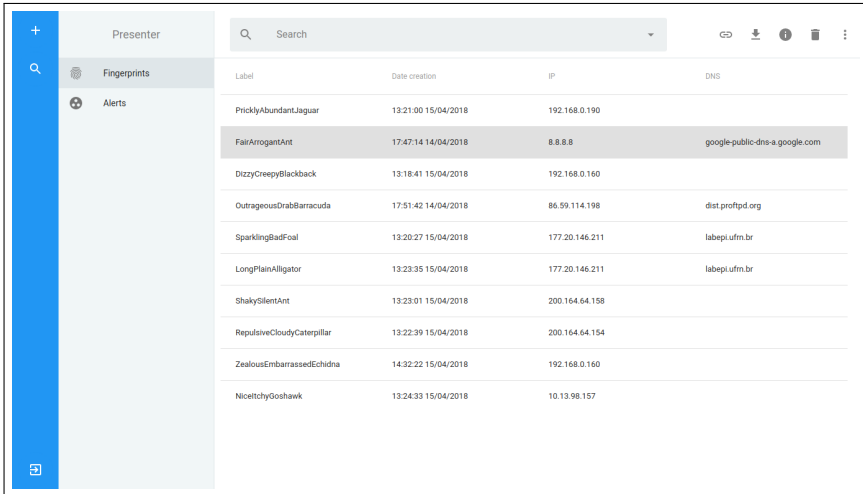
## Componentes e tecnologias desenvolvidas

- ▶ Infraestrutura (Rotas, RTT e Serviços)
- ▶ Relógios (TCP e ICMP)
- ▶ Sistema Operacional (TCP ISN e IP ID)
- ▶ Camada de Aplicação (HTTP, SSH, DNS e FTP)
- ▶ Integração com IDS (Suricata)



# Resultados do Protótipo

## Utilização dos resultados (presenter)



Label	Date creation	IP	DNS
PricklyAbundantJaguar	13:21:00 15/04/2018	192.168.0.190	
<b>FairArrogantAnt</b>	17:47:14 14/04/2018	8.8.8.8	google-public-dns-a.google.com
DizzyCreepyBlackback	13:18:41 15/04/2018	192.168.0.160	
OutrageousDrabBarracuda	17:51:42 14/04/2018	86.59.114.198	dist.proftpd.org
SparklingBadFoil	13:20:27 15/04/2018	177.20.146.211	labepi.ufm.br
LongPlainAlligator	13:23:35 15/04/2018	177.20.146.211	labepi.ufm.br
ShakySilentAnt	13:23:01 15/04/2018	200.164.64.158	
RepulsiveCloudyCaterpillar	13:22:39 15/04/2018	200.164.64.154	
ZealousEmbarrassedEchidna	14:32:22 15/04/2018	192.168.0.160	
NiceltchyGoshawk	13:24:33 15/04/2018	10.13.98.157	

## Utilização dos resultados (infraestrutura)

The screenshot displays a network analysis tool interface. The top navigation bar includes tabs for INFRASTRUCTURE, SURICATA, CLOCK SKEW, HTTP, SSH, DNS, and FTP. The left sidebar contains a search icon, a fingerprint icon, and an alerts icon. The main content area is titled 'Traceroute' and shows a path of 9 hops represented by blue dots connected by lines. The IP addresses for the hops are: 192.168.0.1, 172.31.1.1, 192.168.1.254, 198.228.8.241, 172.19.1.13, 200.186.13.161, 87.16.148.10, 72.14.212.213, and 108.170.245.161. The right sidebar is divided into two sections: 'Host info' and 'Traceroute details'. The 'Host info' section displays the following details: Label: FairArrogantAnt, IP: 8.8.8.8, OS: Linux, Sensor: labepi-sensor, Date: 17:47:14 14/04/2018, DNS: google-public-dns-a.google.com, Open ports: 443, 53, and Annotation: Google fingerprint. The 'Traceroute details' section shows a JSON-like structure for the traceroute results, including hop 1 with host 192.168.0.1 and hop 2 with host 192.168.1.254.

Presenter

INFRASTRUCTURE SURICATA CLOCK SKEW HTTP SSH DNS FTP

Fingerprints

Alerts

Traceroute

Host info

Label: FairArrogantAnt

IP: 8.8.8.8

OS: Linux

Sensor: labepi-sensor

Date: 17:47:14 14/04/2018

DNS: google-public-dns-a.google.com

Open ports: 443, 53

Annotation

Google fingerprint

Traceroute details

```
"Traceroute": { 9 items
  "1": { 3 items
    "host": "192.168.0.1"
    "protocol": "tcp"
    "rtt": 0.0058746337890625
  }
  "2": { 3 items
    "host": "192.168.1.254"
    "protocol": "tcp"
    "rtt": 0.003819704055786133
  }
  "3": { 3 items
```

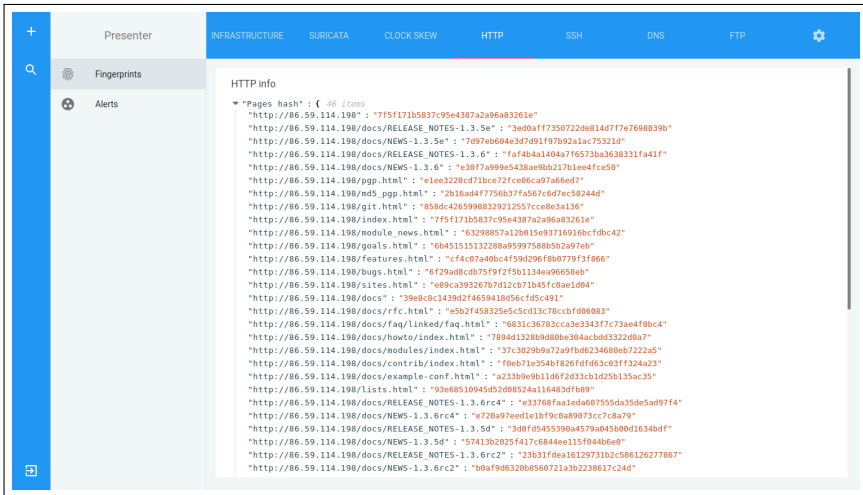
# Resultados do Protótipo

## Utilização dos resultados (Relógio)



# Resultados do Protótipo

## Utilização dos resultados (HTTP)



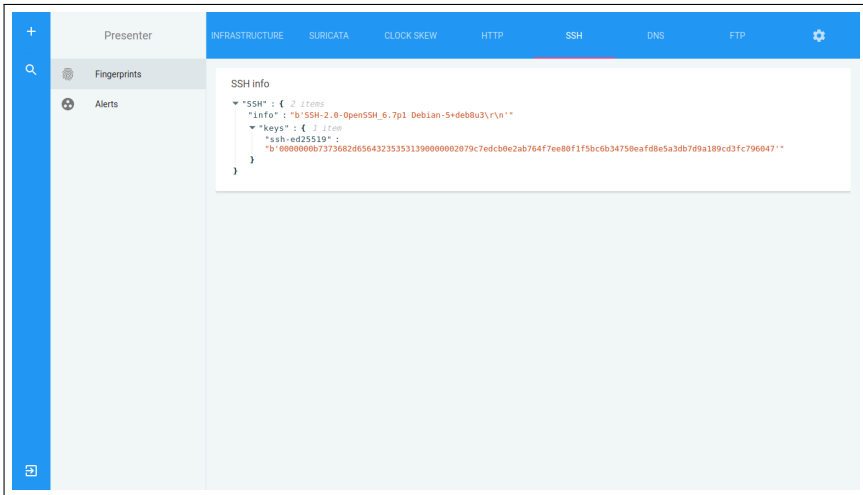
The screenshot displays a web application interface with a navigation menu on the left and a main content area. The navigation menu includes a plus sign, a magnifying glass, and three icons representing Fingerprints, Alerts, and a plus sign. The main content area has a top navigation bar with tabs for INFRASTRUCTURE, SURICATA, CLOCK SKEW, HTTP (selected), SSH, DNS, and FTP. Below the tabs, the 'HTTP info' section is expanded, showing a list of 46 items under the heading 'Pages hash'. Each item is a URL followed by a hash value in quotes.

```
HTTP info
▼ "Pages hash" : { 46 items
  "http://86.59.114.198" : "7f5f171b5837c95e4387a2a96a83261e"
  "http://86.59.114.198/docs/RELEASE_NOTES-1.3.5e" : "3ed0aff7350722de814d7f7e7698039b"
  "http://86.59.114.198/docs/NEWS-1.3.5e" : "7d97eb604e3d7d91f97b92alac75321d"
  "http://86.59.114.198/docs/RELEASE_NOTES-1.3.6" : "faf4b4a1404a7f6573ba3638331fa41f"
  "http://86.59.114.198/docs/NEWS-1.3.6" : "e30f7a999e5438ae9bb217b1ee4fce50"
  "http://86.59.114.198/pgp.html" : "e1ee3220cd71bce72fce06ca97a66ed7"
  "http://86.59.114.198/md5_pgp.html" : "2b16ad4f7756b37fa567c6d7ec50244d"
  "http://86.59.114.198/git.html" : "B58dc42659988329212557cce8e3a136"
  "http://86.59.114.198/index.html" : "7f5f171b5837c95e4387a2a96a83261e"
  "http://86.59.114.198/module_news.html" : "63298857a12b015e93716916bcfdb42"
  "http://86.59.114.198/goals.html" : "6b451515132288a95997588b5b2a97eb"
  "http://86.59.114.198/features.html" : "cf4c07a40bc4f59d296f8b0779f3f866"
  "http://86.59.114.198/bugs.html" : "6f29ad8cdb75f92f5b1134ea96658eb"
  "http://86.59.114.198/sites.html" : "e89ca393267b7d12cb71b45fc0ae1d04"
  "http://86.59.114.198/docs" : "39e8c8c1439d2f4659418d56cfd5c491"
  "http://86.59.114.198/docs/rfc.html" : "e5b2f458325e5c5cd13c78ccbf06083"
  "http://86.59.114.198/docs/faq/linked/faq.html" : "6831c36783cca3e3343f7c73ae4f0bc4"
  "http://86.59.114.198/docs/howto/index.html" : "7894d1328b9d80be304acbdd3322d0a7"
  "http://86.59.114.198/docs/modules/index.html" : "37c3029b9a72a9fbd6234680eb7222a5"
  "http://86.59.114.198/docs/contrib/index.html" : "f0eb71e354bf826dfd63c03ff324a23"
  "http://86.59.114.198/docs/example-conf.html" : "a233b9e9b11df62d33cb1d25b135ac35"
  "http://86.59.114.198/lists.html" : "93e68510945d52d08524a116483dfb89"
  "http://86.59.114.198/docs/RELEASE_NOTES-1.3.6rc4" : "e33768faaleda607555da35de5ad97f4"
  "http://86.59.114.198/docs/NEWS-1.3.6rc4" : "e720a97eed1ebf9c0a89073cc7ca79"
  "http://86.59.114.198/docs/RELEASE_NOTES-1.3.5d" : "3d0fd5455390a4579a045b00d1634bdf"
  "http://86.59.114.198/docs/NEWS-1.3.5d" : "57413b2025f417c6844ee115f044b6e0"
  "http://86.59.114.198/docs/RELEASE_NOTES-1.3.6rc2" : "23b31fdea16129731b2c586126277867"
  "http://86.59.114.198/docs/NEWS-1.3.6rc2" : "b0af9d6320b8560721a3b2238617c24d"
```



# Resultados do Protótipo

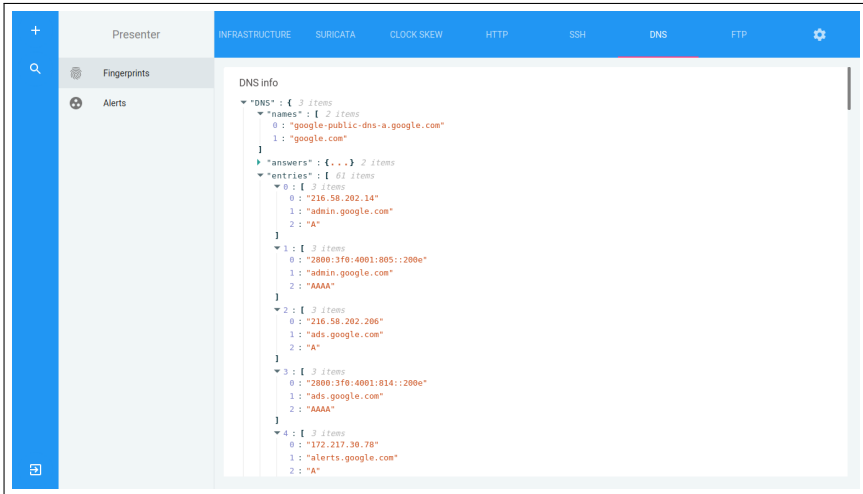
## Utilização dos resultados (SSH)



The screenshot displays a web application interface with a blue sidebar on the left and a main content area. The sidebar contains a search icon, a plus icon, and a minus icon. The main content area has a top navigation bar with tabs for INFRASTRUCTURE, SURICATA, CLOCK SKEW, HTTP, SSH (selected), DNS, and FTP, along with a settings gear icon. Below the navigation bar, the 'SSH' tab is active, showing 'SSH info' with a tree view of JSON data. The data includes 'info' and 'keys' fields, with the 'keys' field containing a single item with an 'ssh-ed25519' key and a long hexadecimal value.

```
SSH info
└─ SSH: { 2 items
  info: "b'SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u3\r\n"
  keys: { 1 item
    ssh-ed25519:
      b'0000000b7373682d656432353531390000002079c7edcb0e2ab764f7ee80f1f5bc6b34750eafd8e5a3db7d9a189cd3fc796047'
```

## Utilização dos resultados (DNS)

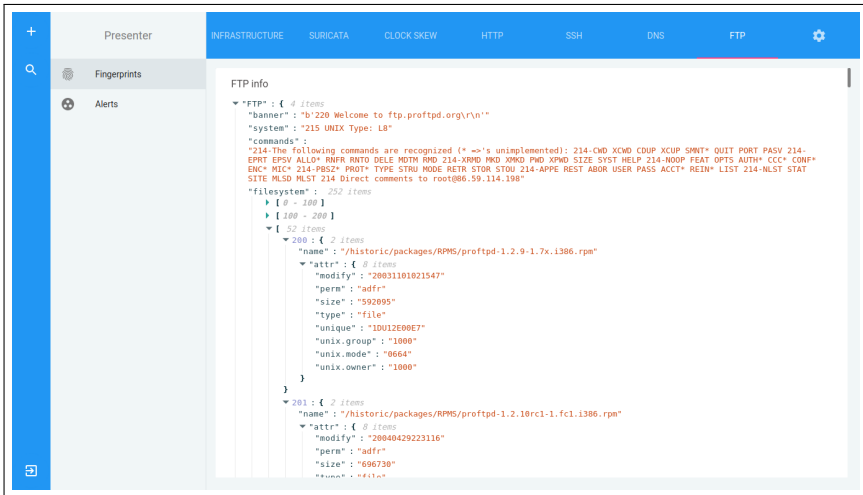


The screenshot shows a web application interface with a blue sidebar on the left and a main content area. The sidebar contains a plus sign, a magnifying glass, and icons for 'Fingerprints' and 'Alerts'. The main content area has a blue header with tabs for 'INFRASTRUCTURE', 'SURICATA', 'CLOCK SKEW', 'HTTP', 'SSH', 'DNS' (selected), and 'FTP'. Below the header, the 'DNS info' section displays a tree view of JSON data:

```
DNS info
└─ "DNS": { 3 items
  └─ "names": [ 2 items
    0 : "google-public-dns-a.google.com"
    1 : "google.com"
  ]
  └─ "answers": {...} 2 items
  └─ "entries": [ 61 items
    0 : [ 3 items
      0 : "216.58.202.14"
      1 : "admin.google.com"
      2 : "A"
    ]
    1 : [ 3 items
      0 : "2800:3f0:4001:805::200e"
      1 : "admin.google.com"
      2 : "AAAA"
    ]
    2 : [ 3 items
      0 : "216.58.202.206"
      1 : "ads.google.com"
      2 : "A"
    ]
    3 : [ 3 items
      0 : "2800:3f0:4001:814::200e"
      1 : "ads.google.com"
      2 : "AAAA"
    ]
    4 : [ 3 items
      0 : "172.217.36.78"
      1 : "alerts.google.com"
      2 : "A"
    ]
  ]
}
```

# Resultados do Protótipo

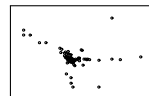
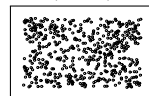
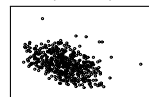
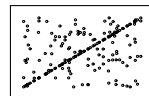
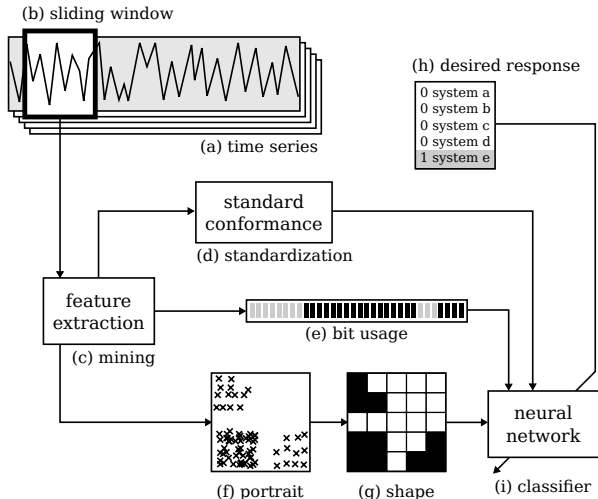
## Utilização dos resultados (FTP)



The screenshot displays a web application interface for analyzing scan results. The top navigation bar includes categories like INFRASTRUCTURE, SURICATA, CLOCK SKEW, HTTP, SSH, DNS, and FTP. The left sidebar shows 'Fingerprints' and 'Alerts' sections. The main content area, titled 'FTP info', shows a detailed JSON output of an FTP scan. The output includes the banner, system type, supported commands, and a list of files found in the filesystem, such as RPM packages for proftpd.

```
FTP info
{
  "FTP": {
    "items": 4
  }
}
{
  "banner": "b'220 Welcome to ftp.proftpd.org\r\n\"",
  "system": "215 UNIX Type: L8",
  "commands": "214-The following commands are recognized (* ->'s unimplemented): 214-CMD XCWD CDUP XCPU SMNT* QUIT PORT PASV 214-EPRT EPSV ALLO* RNFR RNTD DELE MDTM RMD 214-XRMD MKD XMKD PWD XPWD SIZE SYST HELP 214-NOOP FEAT OPTS AUTH* CCC* CONF* ENC* MIC* 214-PBSZ* PROT* TYPE STRU MODE RETR STOR STOU 214-APPE REST ABOR USER PASS ACCT* REIN* LIST 214-NLST STAT SITE MLSD HLST 214 Direct comments to root@86.59.114.198",
  "filesystem": {
    "items": 252
  }
}
{
  "items": 2
}
{
  "items": 2
}
{
  "items": 52
}
{
  "items": 2
}
{
  "name": "/historic/packages/RPMS/proftpd-1.2.9-1.7x.i386.rpm",
  "attr": {
    "items": 8
  }
}
{
  "modify": "20031101021547",
  "perm": "adfr",
  "size": "592095",
  "type": "file",
  "unique": "10U12E00E7",
  "unix.group": "1000",
  "unix.mode": "0664",
  "unix.owner": "1000"
}
{
  "items": 2
}
{
  "name": "/historic/packages/RPMS/proftpd-1.2.10rc1-1.fc1.i386.rpm",
  "attr": {
    "items": 8
  }
}
{
  "modify": "20040429223116",
  "perm": "adfr",
  "size": "696730",
  "type": "file"
}
```

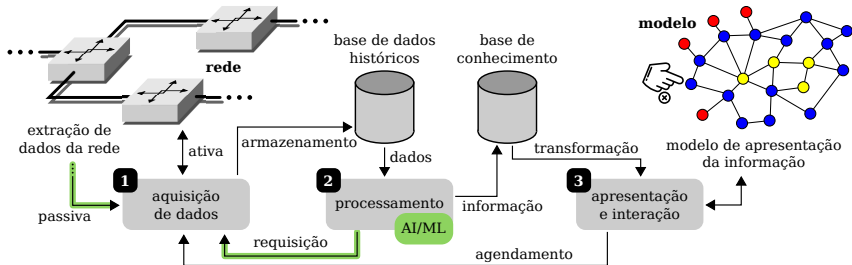
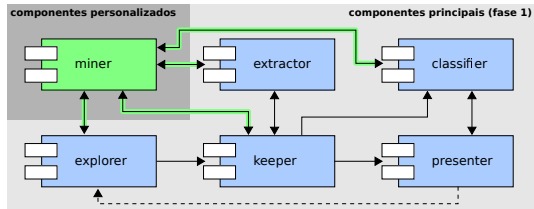
## Utilização dos resultados (Sistema Operacional)



# Proposta para Fase Piloto

## Visão para próxima fase

- ▶ Caracterização passiva
- ▶ Caracterizar infraestrutura
- ▶ Alertar atividade suspeita
- ▶ Confiabilidade da identificação
- ▶ Base de dados e transmissão segura



# 19º WRNP

Workshop RNP

7 | 8 MAIO

Campos do Jordão | SP

Obrigado

João Paulo de Souza Medeiros

[jpsm@dct.ufrn.br](mailto:jpsm@dct.ufrn.br)



RNP

MINISTÉRIO DA  
DEFESA

MINISTÉRIO DA  
CULTURA

MINISTÉRIO DA  
SAÚDE

MINISTÉRIO DA  
EDUCAÇÃO

MINISTÉRIO DA  
CIÊNCIA, TECNOLOGIA,  
INOVAÇÕES E COMUNICAÇÕES

