18º WRNP
Workshop RNP
15 | 16 MAIO
Belém | PA

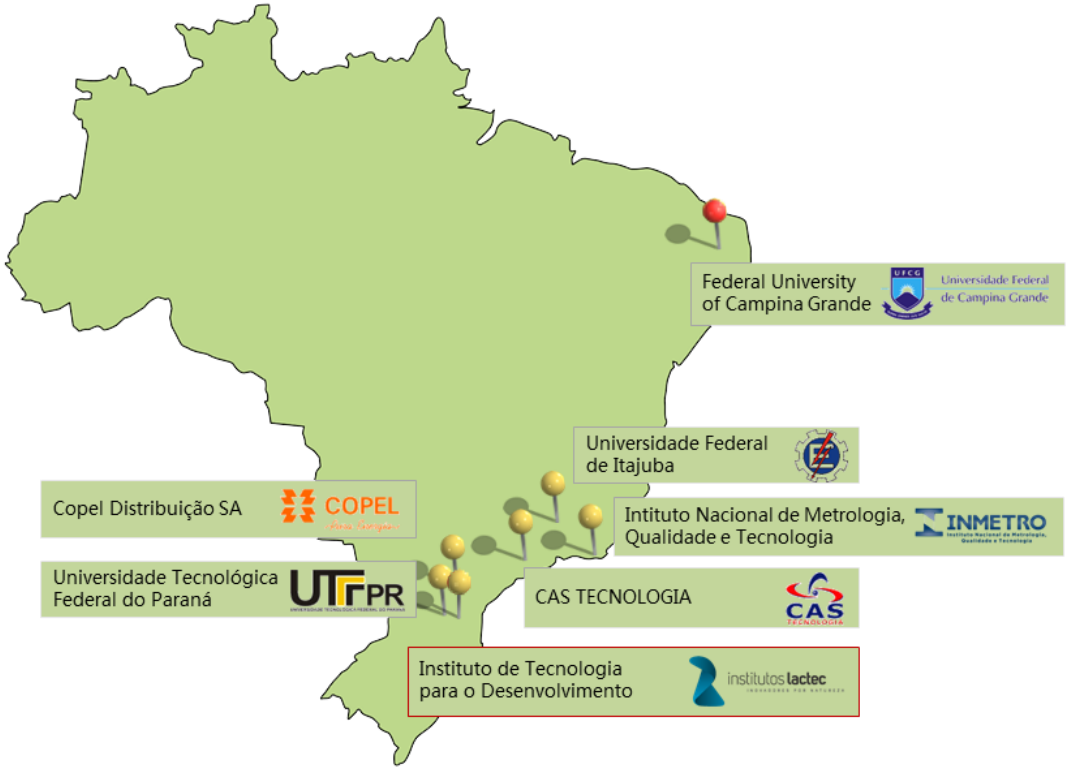
SecureCloud – Processamento Seguro de Big Data em Nuvens Não-Confiáveis

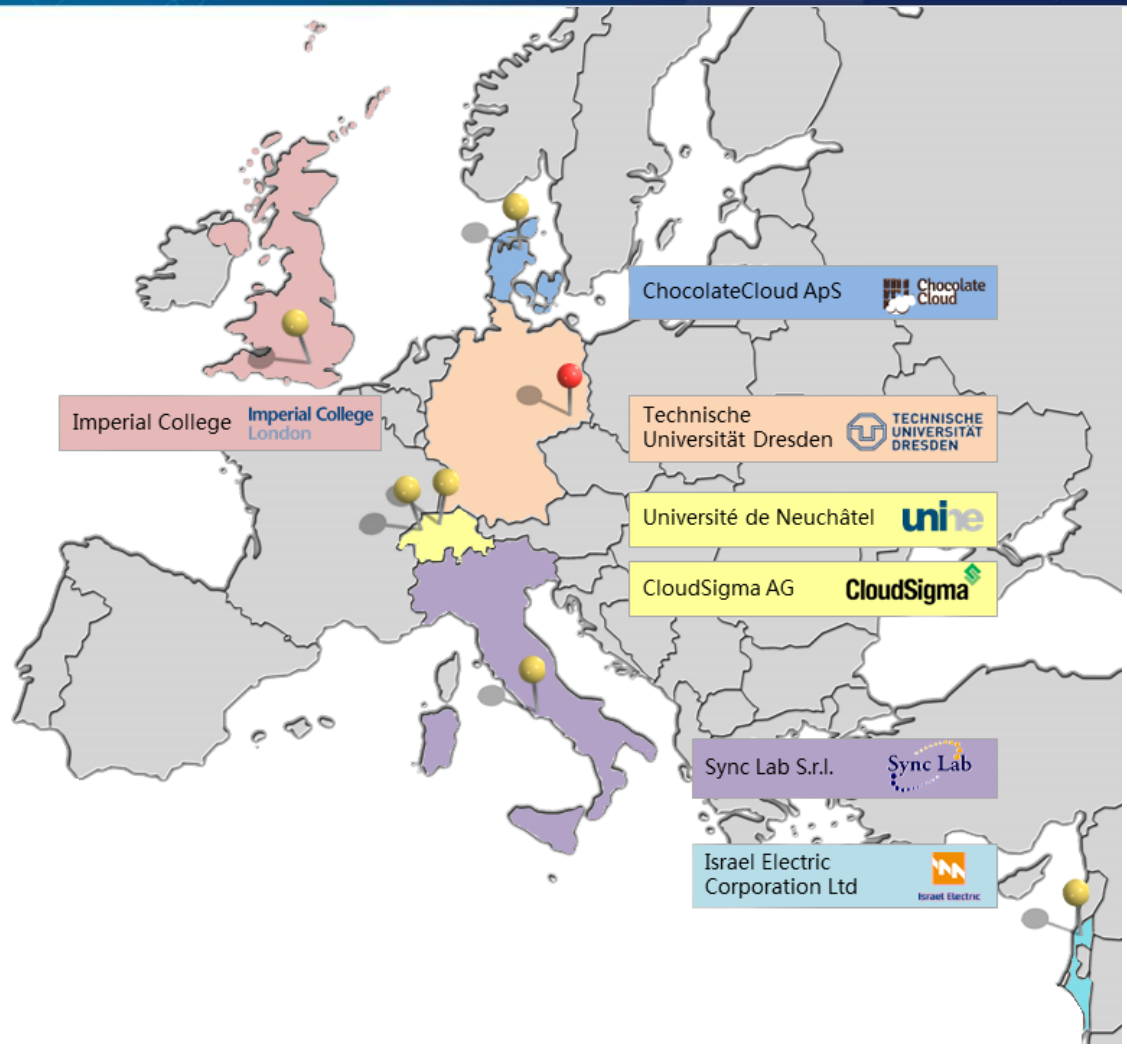
Andrey Brito

Universidade Federal de Campina Grande

SecureCloud – Processamento Seguro de Big Data em Nuvens Não-Confiáveis

Parceiros





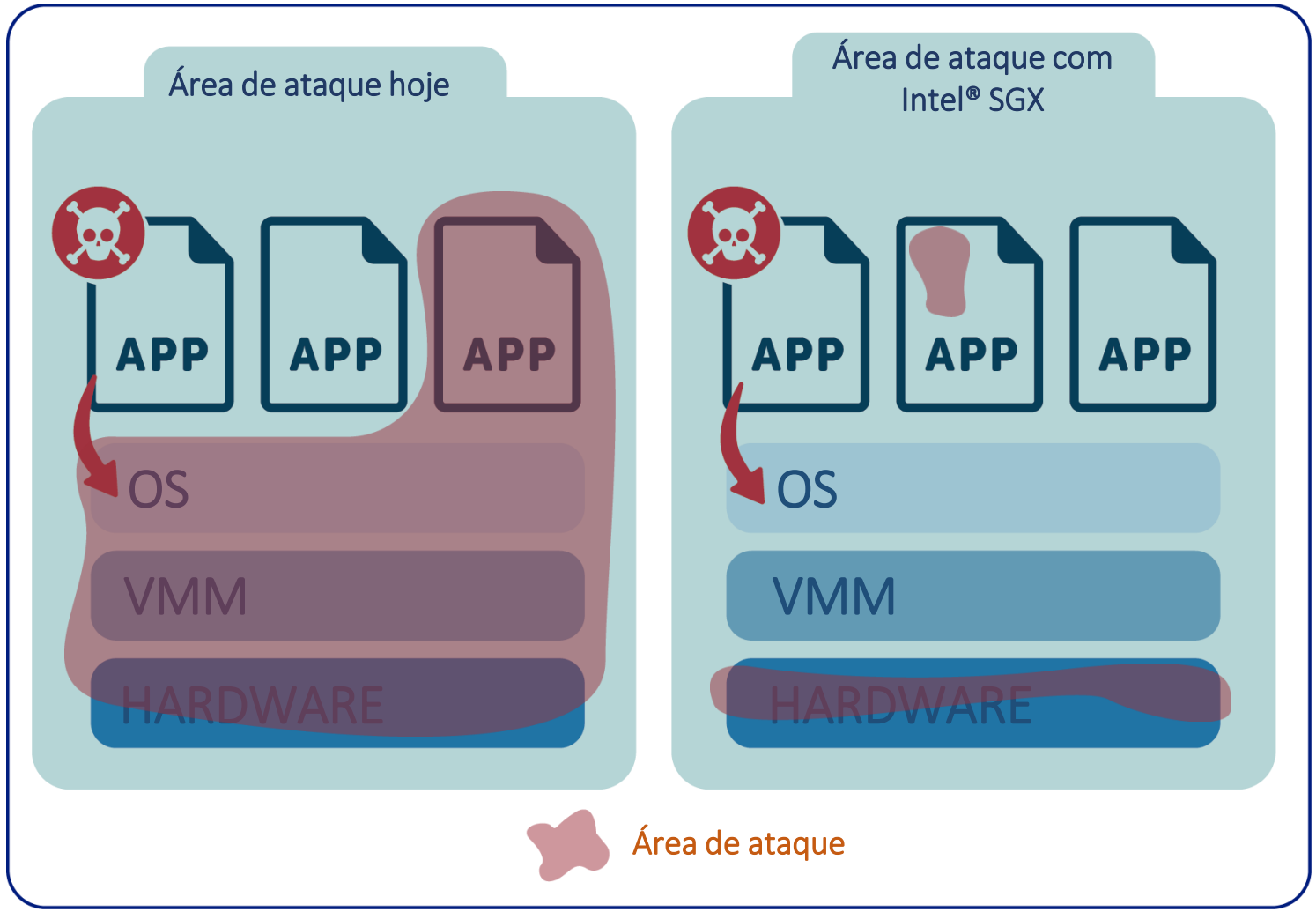
SecureCloud

Objetivo principal: aumentar a confidencialidade de programas executando na nuvem.

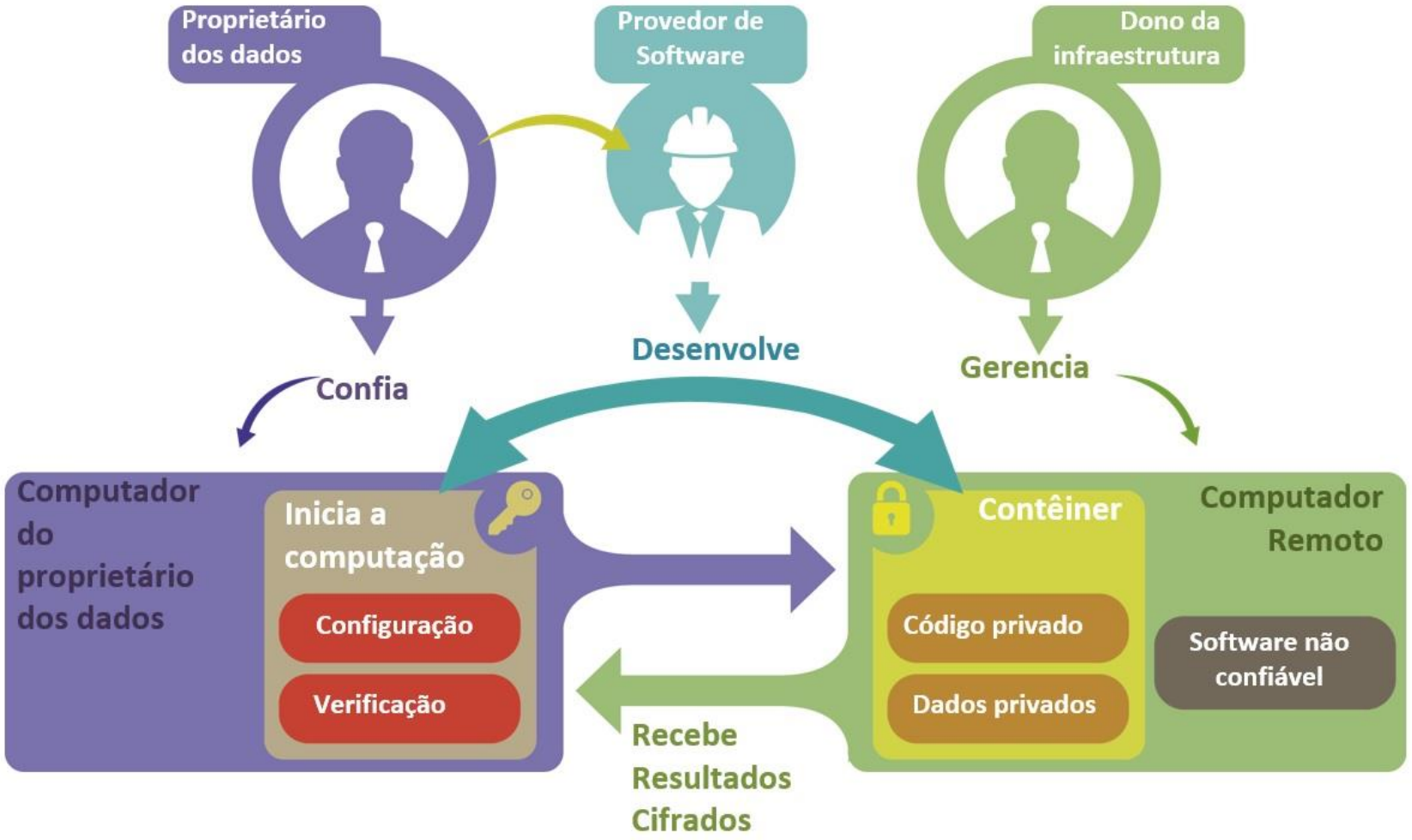
Abordagem: se/como mecanismos de segurança em hardware de CPUs comuns (em especial, Intel SGX) podem ajudar a aumentar a confidencialidade de programas.

Uma vez que os proprietários dos dados não precisem mais confiar nos desenvolvedores da aplicação ou no provedor de nuvem para proteger com seus dados, estará criado um ambiente para aplicações inovadoras que usem dados críticos

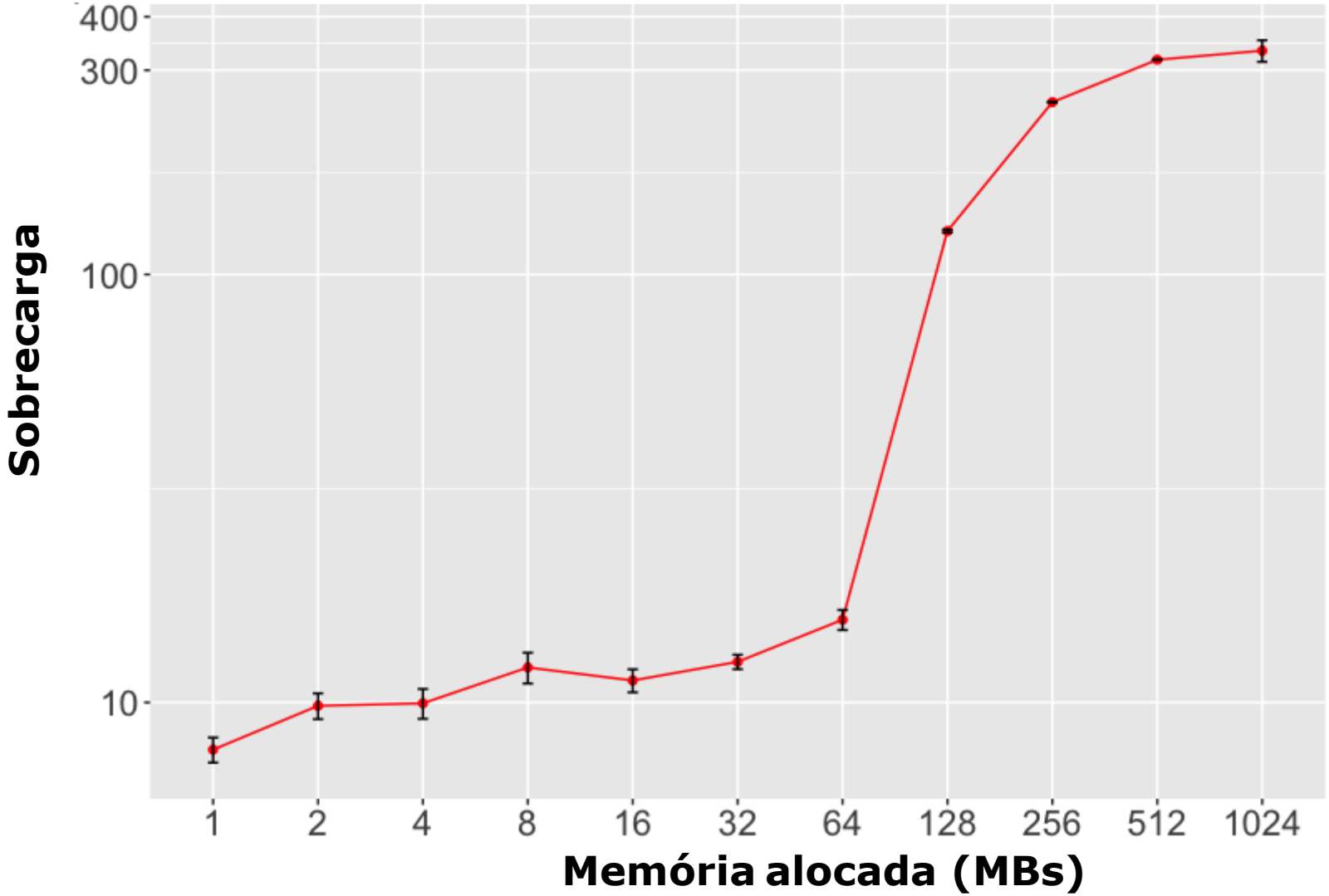
Desafio: Excesso de Software



Proteção com enclaves



Desafio: Usabilidade e Desempenho



Resultados principais (Mês 16)

Suporte para geração de contêineres seguros a partir de código-fonte não modificado.

Middleware de comunicação indireta (Pub/Sub) com proteção de privacidade.

Biblioteca para detecção de integridade em aplicações não SGX.

Integração de sensores comuns com aplicações confiáveis na nuvem.

Modelos de aplicações e arquiteturas para aplicações que garantam segurança e privacidade de dados sensíveis.

Impacto esperado

Setor produtivo:
- Redução da barreira de adoção de computação na nuvem.
- Incentivo ao desenvolvimento de aplicações que usem dados sensíveis (ex., IoT).
- Redução das barreiras para troca de serviços de nuvem entre países.

Academia:
- Novas ferramentas para a solução de problemas complexos de gerência de privacidade e segurança.

Sociedade:
- Maior proteção de dados pessoais.

Resultados principais (Mês 16)

EuroSys'17 - *SGXBounds: Memory Safety for Shielded Execution*

SAC'17 *- Security and Privacy Preserving Data Aggregation in Cloud Computing*

DATE'17 *- SecureCloud: Secure Big Data Processing in Untrusted Clouds*

PDP'17 - *Cloudifying Critical Applications: a Use Case from the Power Grid Domain*

OSDI'16 *- SCONE: Secure Linux Containers with Intel SGX*

Middleware'16 *- Secure Content-Based Routing Using Intel Software Guard Extensions*

HOST'16 *- Machine Learning Resistant Strong PUF: Possible or Pipe Dream?*

ICT4S'16 *- Encouraging Renewable Energy Consumption Through Dynamic Pricing*

IFIP SEC'16 *- Multicast Delayed Authentication For Streaming Synchrophasor Data in the Smart Grid*

SBSEG'16 *- Privacy-Preserving Techniques in Smart Metering: An Overview*

SBSEG'16 *- Agregação de dados na nuvem com garantias de segurança e privacidade*

Próximos passos

Gerência e orquestração de aplicações seguras complexas.

Integração com plataformas e ferramentas de nuvem.

Validação de arquiteturas que reduzam a complexidade e o overhead.

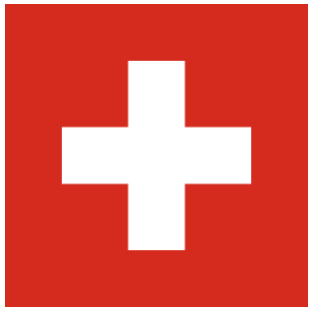
Serviços de plataforma para construção de aplicações de big data que sejam seguras e amigáveis para a nuvem.

O projeto SecureCloud é financiado através da 3ª chamada coordenada Brasil-Europa.

Comissão Europeia
Horizon 2020

Brasil
Governo Federal
MCTIC – RNP – CTIC

Suíça
Secretaria Estatal para Educação,
Pesquisa e Inovação



18º WRNP
Workshop RNP
15 | 16 MAIO
Belém | PA

RNP
MINISTÉRIO DA DEFESA
MINISTÉRIO DA CULTURA
MINISTÉRIO DA SAÚDE
MINISTÉRIO DA EDUCAÇÃO
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES
BRASIL GOVERNO FEDERAL

Obrigado!

Andrey Brito

andrey@computacao.ufcg.edu.br