



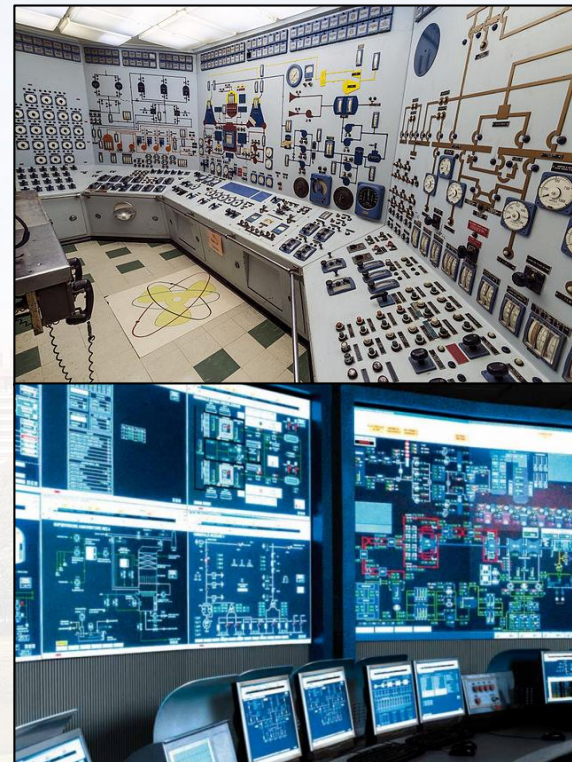
Segurança Cibernética na CHESF: Análise de Vulnerabilidades na Arquitetura, Supervisório SAGE e Protocolos Utilizados no SPCS das Subestações

GPC – Pablo Mascarenhas



- Mudança de paradigma: dependência de software e redes de comunicação
- Protocolos conhecidos: Ethernet, TCP/IP, SSH, NTP, RSTP, ...
- Interoperabilidade: GOOSE, SV, MMS
- Sistema proprietário para aberto (SAGE Linux)

Redução de custos, integração e interoperabilidade não permite “segurança por obscurantismo”



Ooops, your files have been encrypted!
English ▼



What Happened to My Computer?

Your important files are encrypted. Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time. You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay. You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever. We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window. After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT-5 on Mondays-Edm.

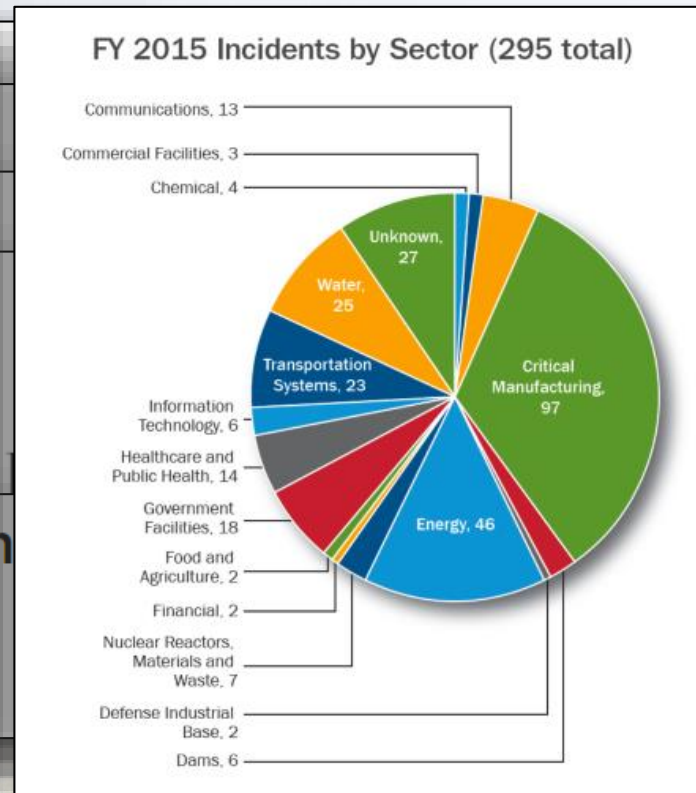
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

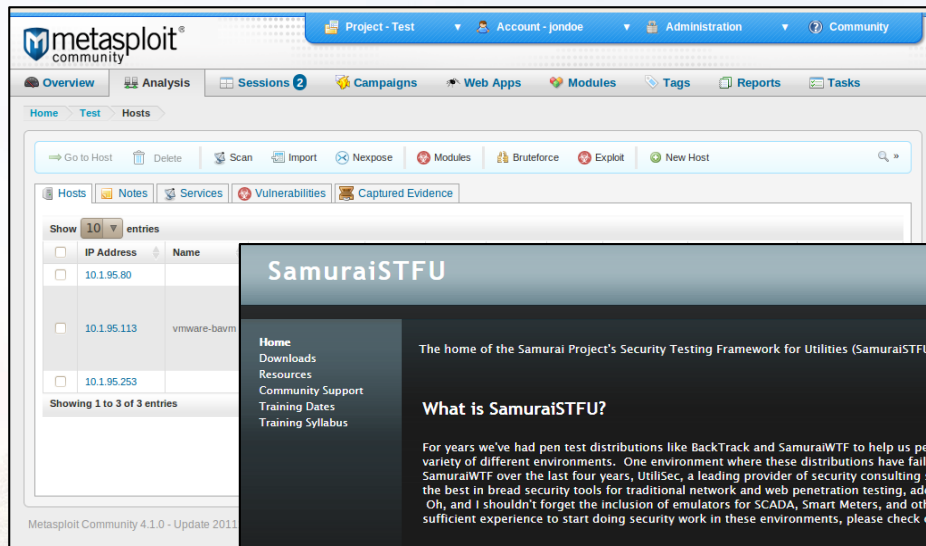
[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)

 **bitcoin**
ACCEPTED HERE

Send \$300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy



- Entender as possíveis formas de ataques
- Estratégias de mitigação
- Ter uma política de segurança cibernética



SamuraiSTFU

Home
Downloads
Resources
Community Support
Training Dates
Training Syllabus

The home of the Samurai Project's Security Testing Framework for Utilities (SamuraiSTFU).

What is SamuraiSTFU?

For years we've had pen test distributions like BackTrack and SamuraiWTF to help us perform penetration testing in most IT env variety of different environments. One environment where these distributions have failed to meet the needs of their users is on SamuraiWTF over the last four years, UtiliSec, a leading provider of security consulting services in the energy sector, has created the best in breed security tools for traditional network and web penetration testing, adds specialized tools for embedded and RT. Oh, and I shouldn't forget the inclusion of emulators for SCADA, Smart Meters, and other types of energy sector systems to provide sufficient experience to start doing security work in these environments, please check out distribution out.

What problems are we trying to address?

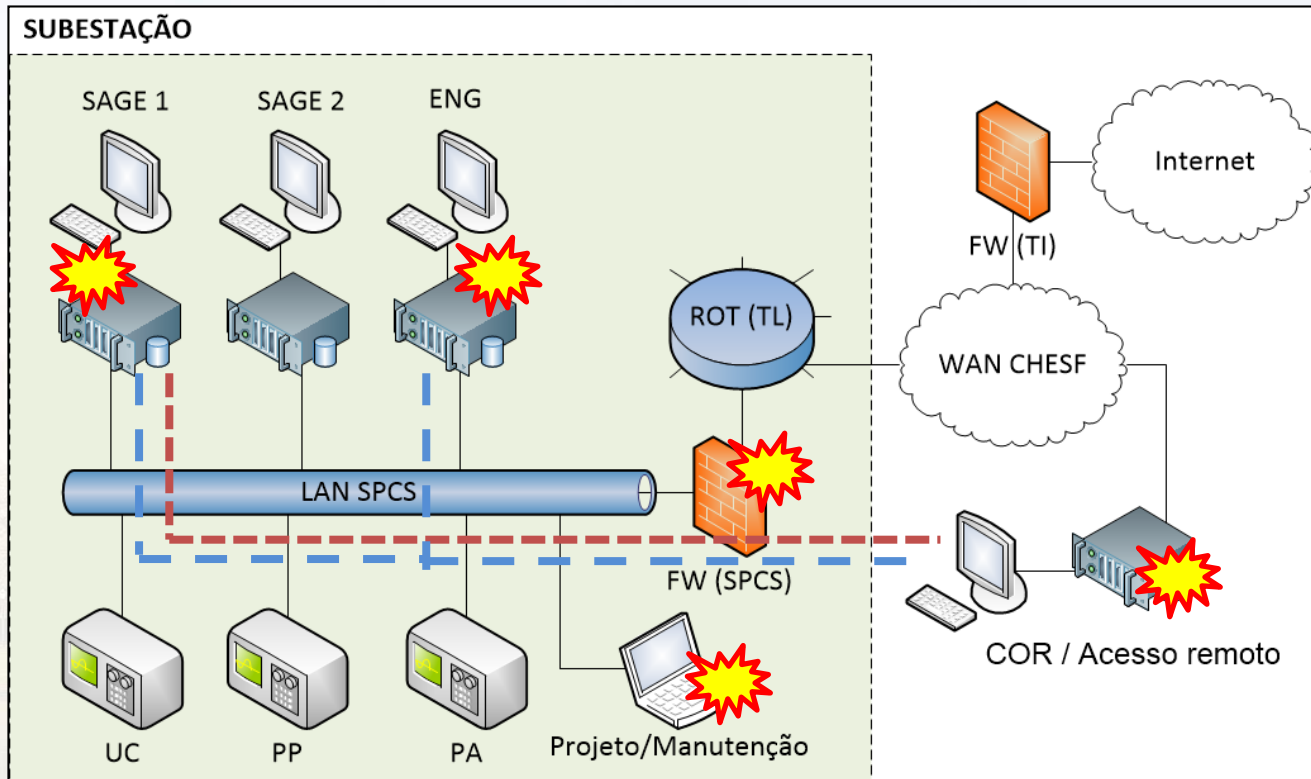
- Not enough people in the energy sector with the necessary knowledge or experience to perform penetration testing
- Many security firms with highly technical staff have the knowledge for 80% of the work, but don't realize it
 - Wired and Wireless Network Testing
 - Web and Traditional Application Testing
 - Embedded Hardware Testing
- The main thing these firms are missing is energy sector context
- Utilities are hesitant to bring in security firms with little control system specific experience
- Few utilities have the in-house expertise and need a greater number of security firms to pick from
- Very few security tools exist to work with control system protocols beyond packet capture and decode

FRONTEIRA DA REDE

- Autenticação falha
- Serviços vulneráveis
- Erro na configuração
- Backdoors
- Bypass
- Pivoteamento

— — — — — DNP3

- SSH, RD, FTP, ...

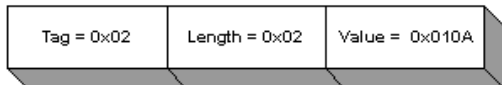
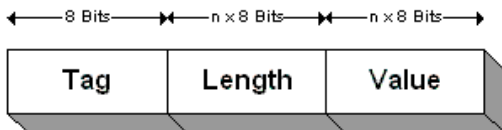
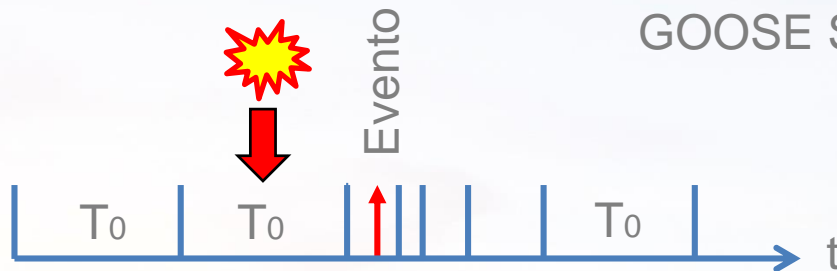


FRONTEIRA DA REDE

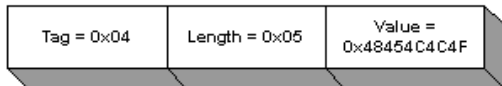
Análise em uma instalação SAGE típica Chesf (CentOS 5.6 SAGE update 23.18)

SEVERIDADE	QUANTIDADE	EXEMPLOS
RELATÓRIO NESSUS VULNERABILITY SCANNER		
CRÍTICA	1	FreeBSD 'telnetd' Daemon Remote Buffer Overflow
MÉDIA	2	Unencrypted Telnet Server; SSH Weak Algorithms Supported
BAIXA	3	SSH Weak MAC Algorithms Enabled; X Server Detection
INFO	20	OS Identification; SSH Server Type and Version Information
RELATÓRIO NEXPOSE COMMUNITY EDITION		
CRÍTICA	2	OpenSSH X11 Cookie Local Authentication Bypass Vulnerability; 'rsh' Remote Shell Service Enabled
SEVERA	14	FTP credentials transmitted unencrypted; Database Open Access; OpenSSL SSL/TLS MITM vulnerability; Unencrypted Telnet Service Available; TLS/SSL Server is enabling the POODLE attack
MODERADA	10	FTP access with ftp account; OpenSSH "X11UseLocalhost" X11 Forwarding Session Hijacking Vulnerability; ICMP timestamp response

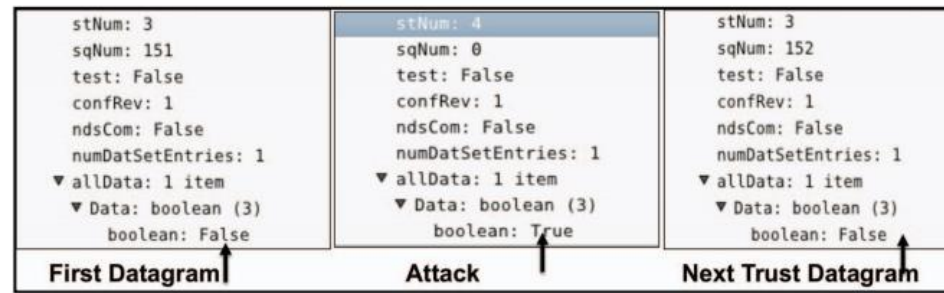
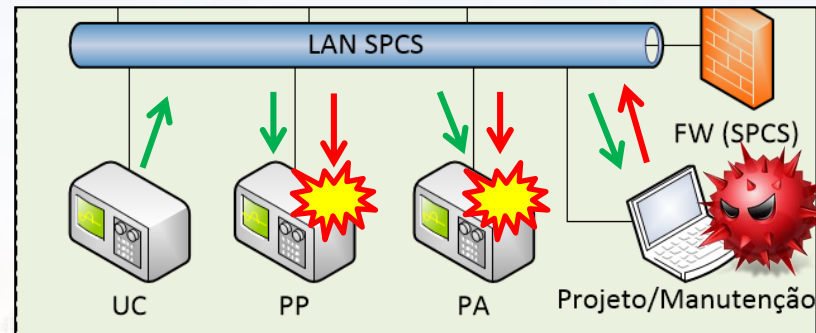
GOOSE SPOOF



Encoding of integer 266 or 0x010A

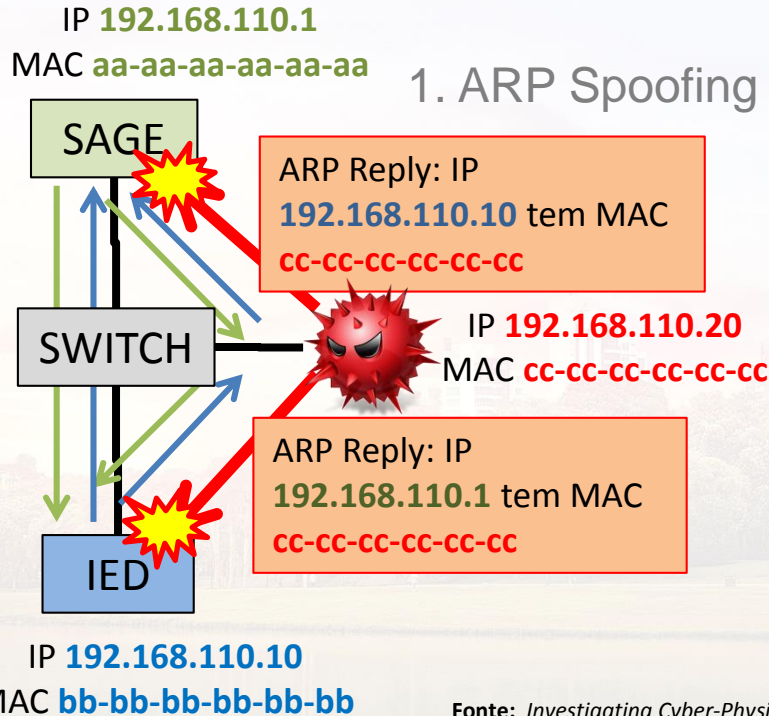


Encoding of string "HELLO" or 0x48454C4C4F



Fonte: Exploiting the GOOSE Protocol: A Practical Attack on Cyber-infrastructure (Hoyos, Juan et al.)

MMS MAN-IN-THE-MIDDLE



2. Sequestro da sessão

```
[TCP Segment Len: 23]
Sequence number: 67      (relative sequence number)
[Next sequence number: 90      (relative sequence number)]
Acknowledgment number: 17 (relative ack number)
Header Length: 20 bytes
[Window size scale: 0]
Checksum: 0x221b
```

```

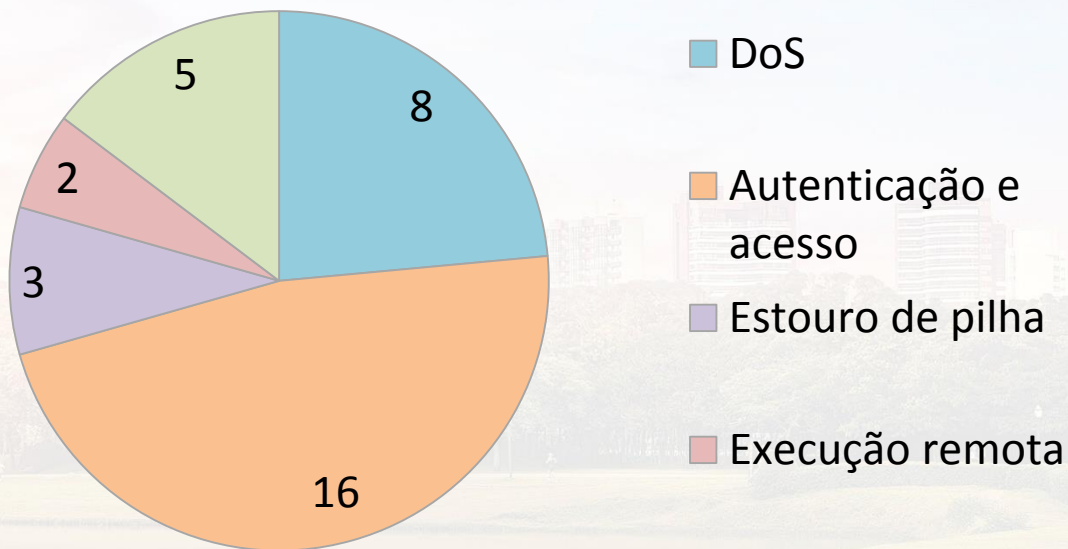
MMS
├─ confirmed-RequestPDU
│   └─ invokeID: 1
├─ confirmedServiceRequest: getNameList (1)
│   └─ getNameList
│       └─ extendedObjectClass: objectClass (0)

```

Fonte: *Investigating Cyber-Physical Attacks against IEC 61850 Photovoltaic Inverter Installations (Kang, B. et al)*

VULNERABILIDADES EM DISPOSITIVOS

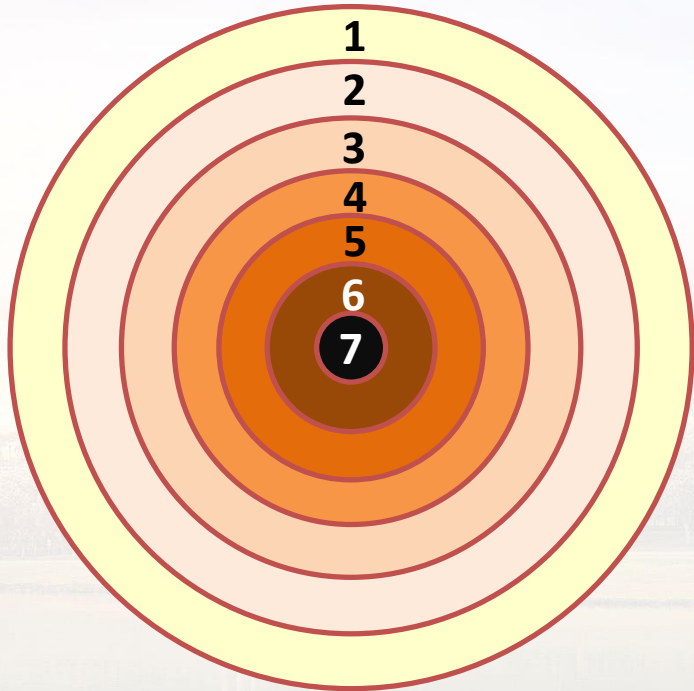
Foram encontradas 34 vulnerabilidades relatadas em produtos (IEDs, switches, softwares de configuração, roteador, etc) comumente usados no SPCS Chesf.



TÓPICO	TI	TO
Antivírus	Comum, facilmente implantado e atualizado	Incomum, pode impactar no desempenho
Vida útil	Normalmente 2-3 anos, várias opções de upgrades	10-20 anos, poucos fabricantes
Patches	Abrangente, automática	Requer cronograma longo e testes
Resposta a incidentes	Facilmente implementada; há requisitos regulatórios	Foca no retorno do ativo à operação; procedimentos não amadurecidos
Teste de segurança	Possui sistemas robustos	Teste customizado

Fonte: *Control Systems Cyber Security: Defense in Depth Strategies (US Department of Homeland Security)*

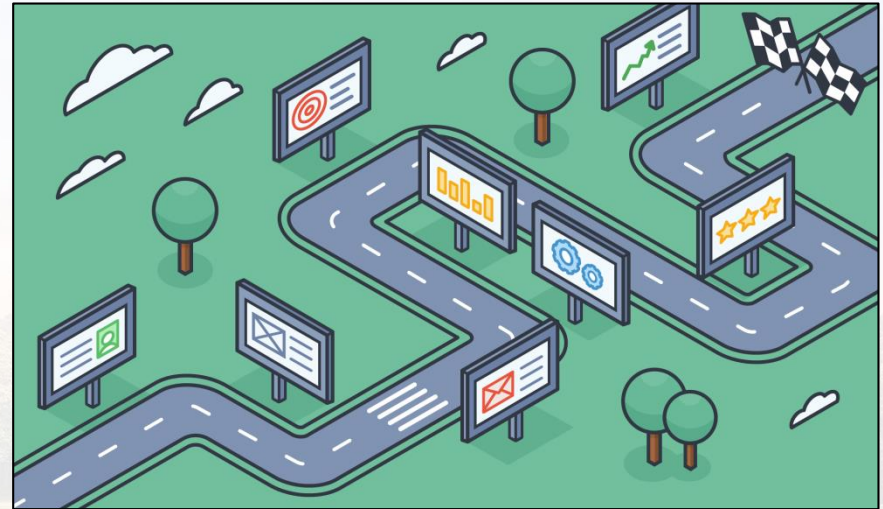
Defesa em Profundidade



1. **Controle de fronteira:** defesa da fronteira com a Internet (IT) e com a rede corporativa
2. **Política de segurança:** treinamento, procedimentos, plano de resposta a incidentes, etc
3. **Arquitetura de rede:** firewall, roteadores, switches, VLANs, DMZ, etc
4. **Protocolos:** MMS, DNP3, etc
5. **Hosts:** sistemas operacionais, atualizações
6. **Aplicação:** bancos de dados, http, sftp, ssh,...
7. **IEDs, UTRs:** patches, senhas, etc

MAPA PARA CRIAÇÃO DE UMA POLÍTICA DE SEGURANÇA ABRANGENTE

- Necessidade para o negócio
- Equipe multidisciplinar (CSIRT)
- Escopo e atribuições
- Procedimentos
- Avaliar ativos críticos
- Gerenciamento de risco e resposta a incidentes
- Treinamento (!!)
- Monitorar e avaliar continuamente




Pablo Mascarenhas de Araújo

 (81) 3229-3456

 (81) 99434-8677

 pablom@chesf.gov.br

 www.chesf.gov.br

Coautores:

Fábio André da Silva

Paulo Ricardo L. de N. Coutinho