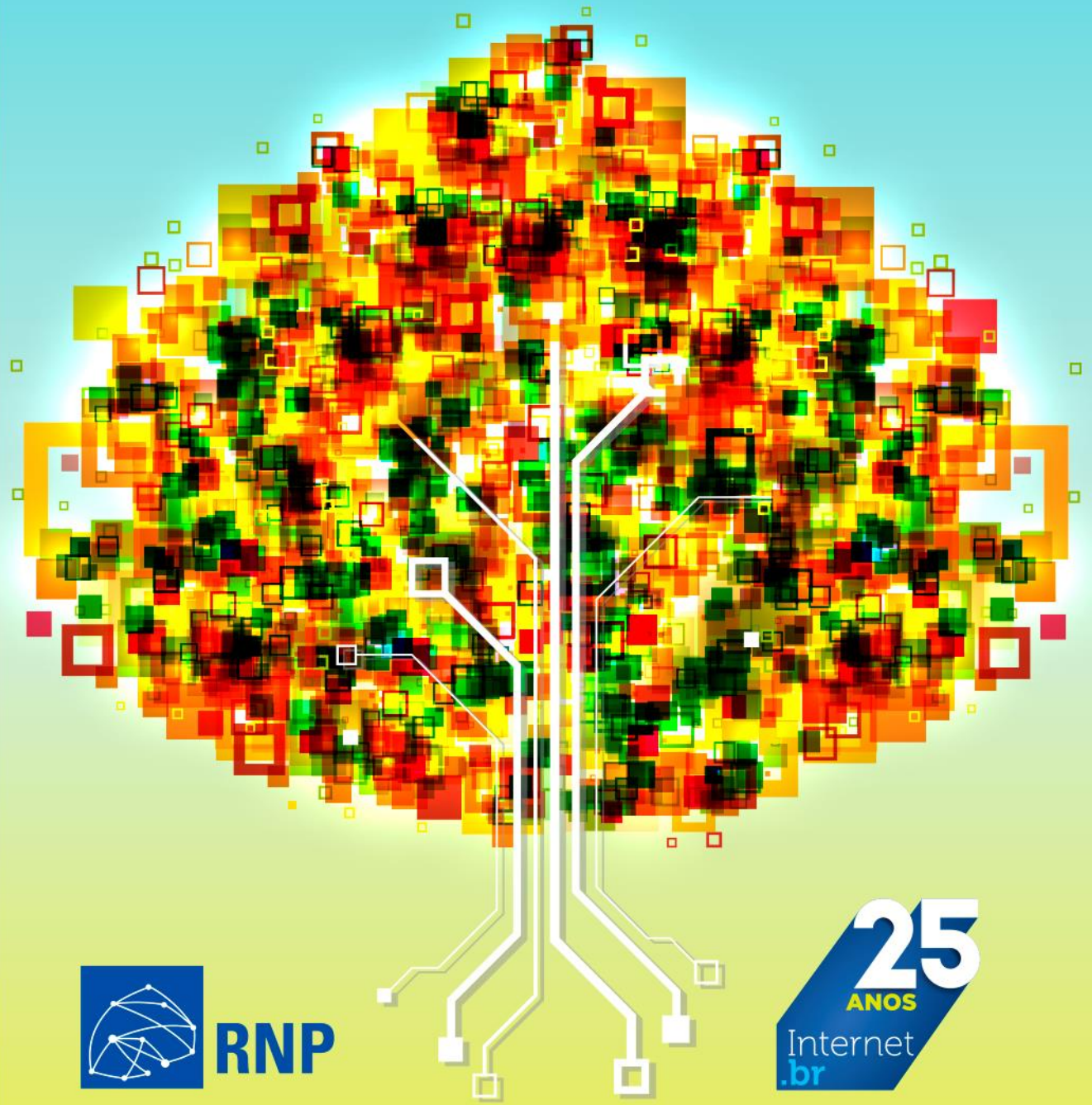


FORUMRNP 2017

25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

Segurança da informação nos campi: desafios e tendências

Carla Freitas - RNP

RNP

25 ANOS Internet .br

Cenário da TIC nos campi

Cenário da TIC nos campi

Equipe reduzida

Recursos limitados

Várias TIC dentro da organização

Cenário de TIC nos campi

Grande número de usuários com alta rotatividade

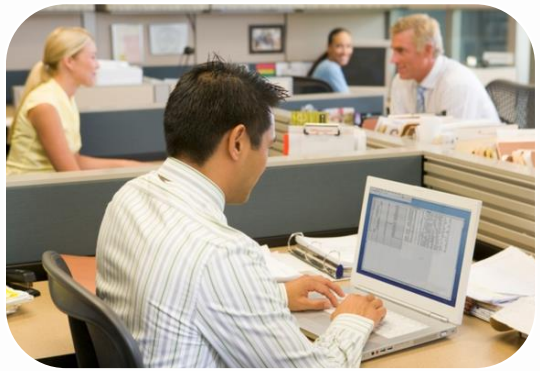
Alto uso de dispositivos móveis

Grande quantidade de computadores

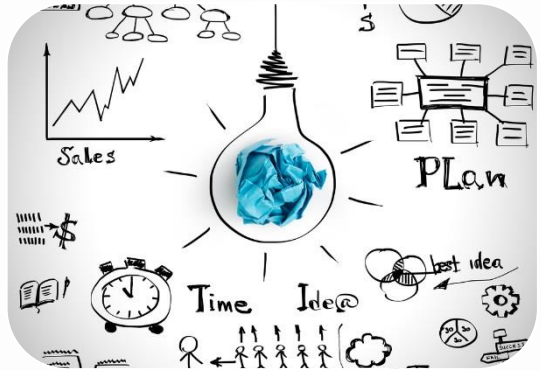
Cenário de TIC nos campi

Diversos softwares e sistemas

Rede com alta capacidade e disponibilidade



Diferentes perfis (visitante, acadêmico e administrativo)



Necessidade de “liberdade” para a pesquisa

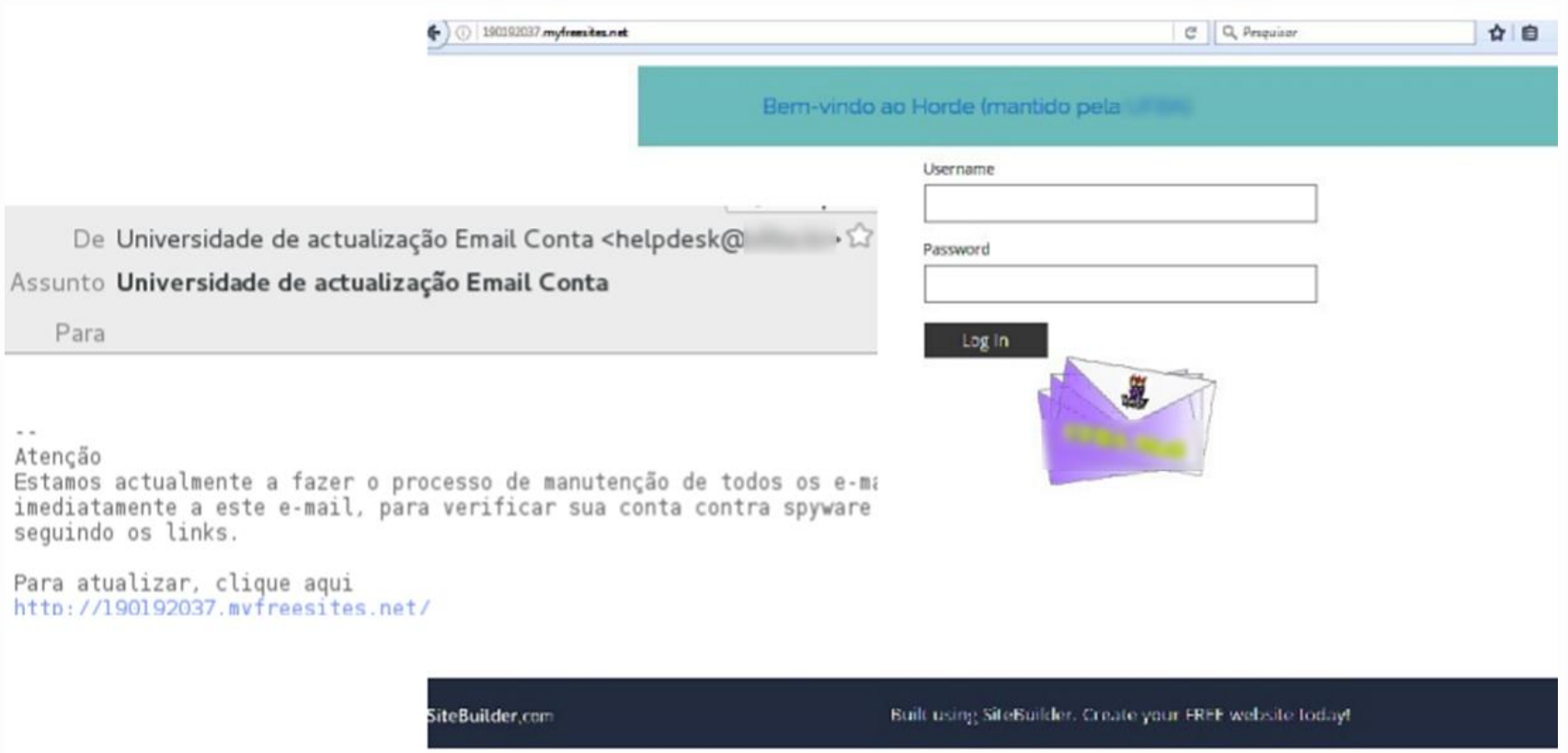
Cenário de TIC nos campi

FORUMRNP 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

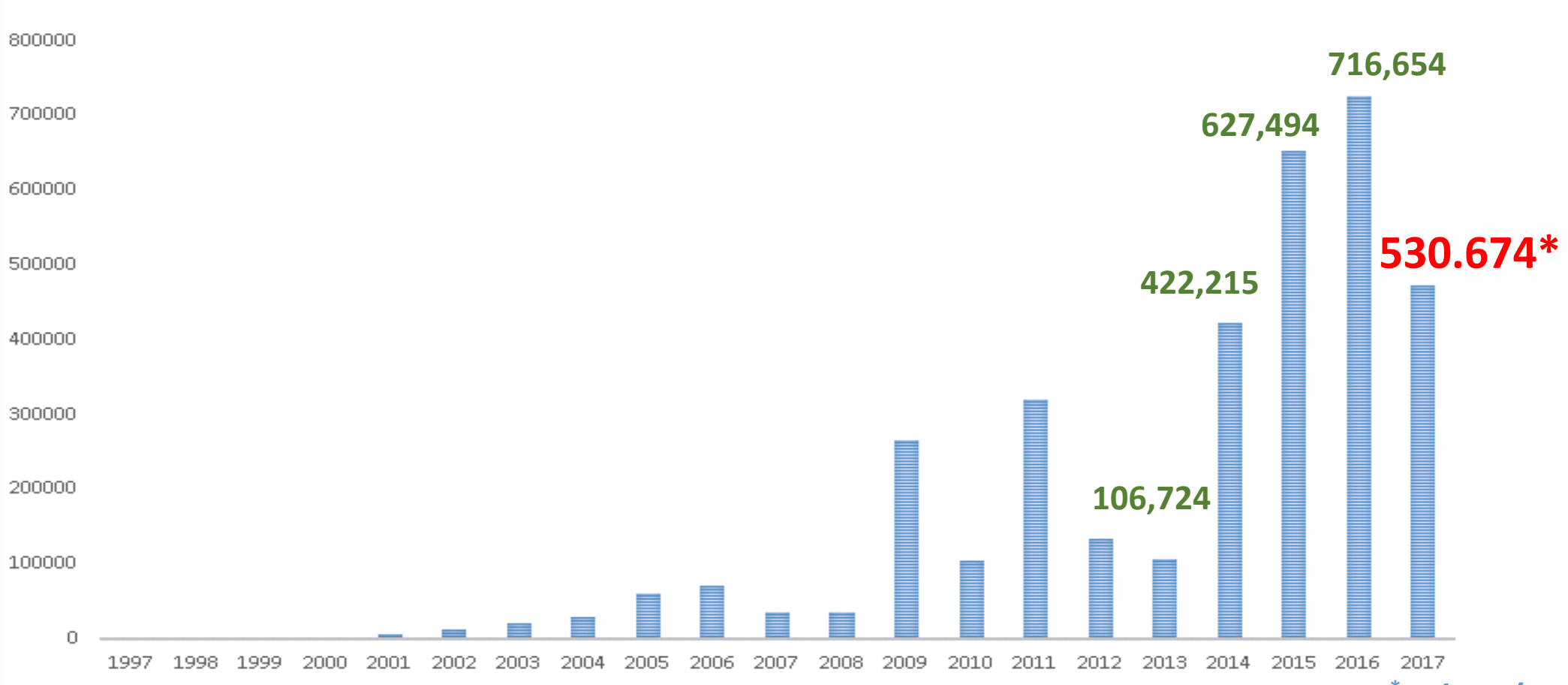
Alvo de ataque: visibilidade, questão política e ambiente propício

```
HacKed [ White Hat Hacker]

Persian Gulf Forever ;)
```

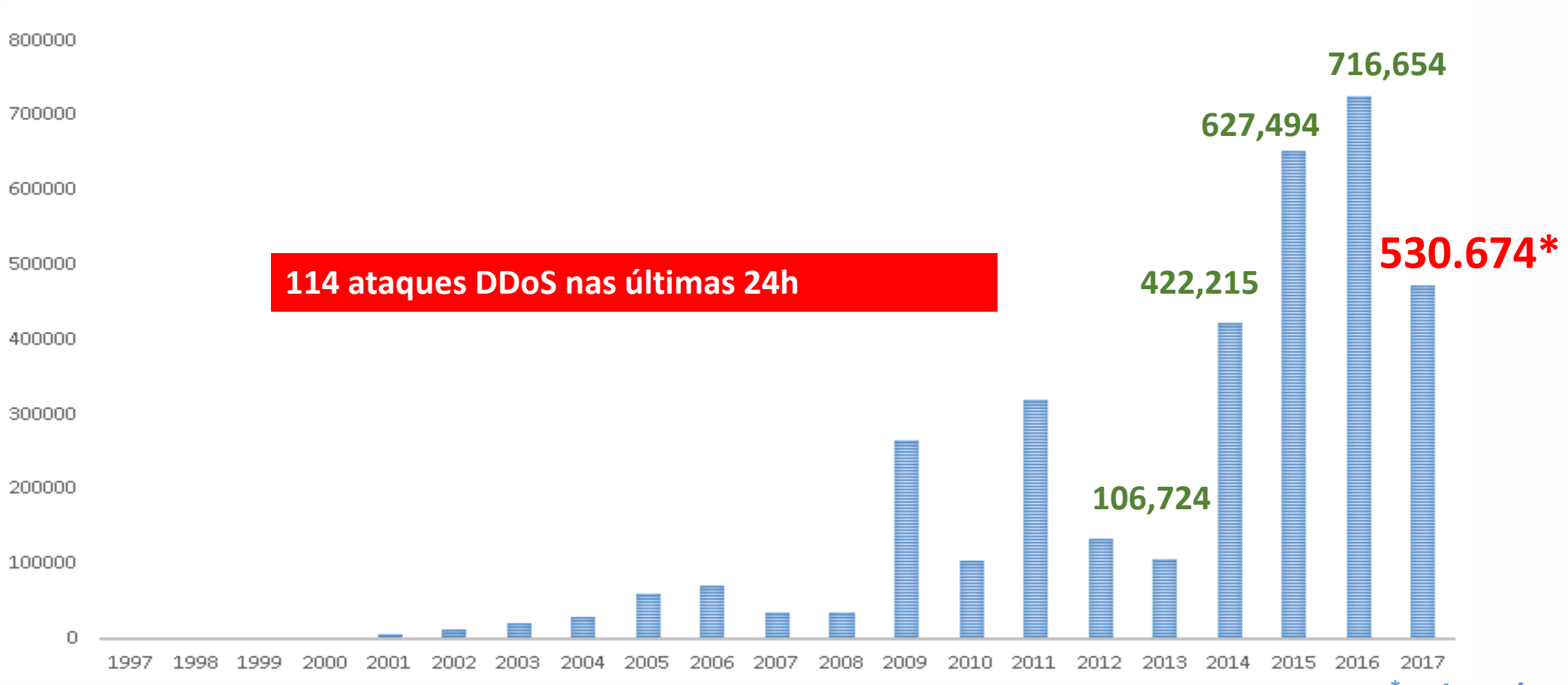


Alvo de ataque: visibilidade, questão política e ambiente propício



*Até Set/2017

Alvo de ataque: visibilidade, questão política e ambiente propício

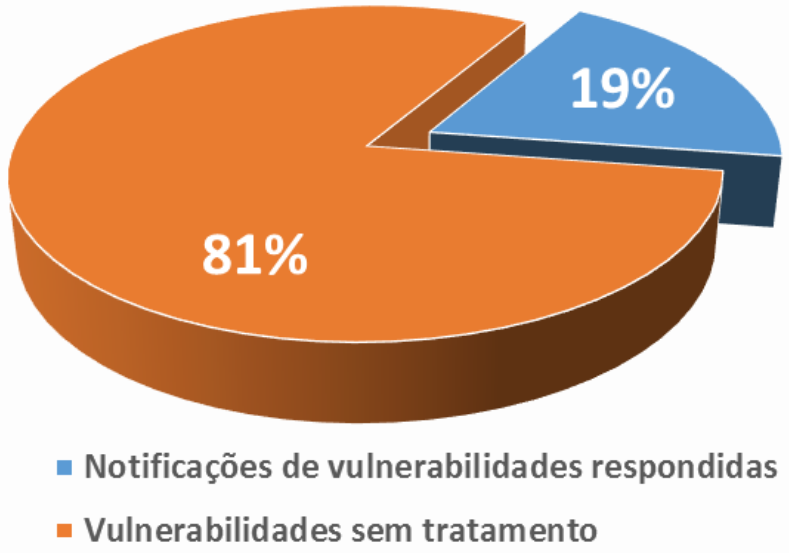


*Até Set/2017

Cenário de TIC nos campi

FORUMRNP 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

Alvo de ataque: visibilidade, questão política e ambiente propício



*Período: Set/2016 a Set/2017

86,4% dos incidentes tem como origem um cliente

Segurança da informação nos campi: desafios e tendências

Desafios

- Dispor de equipe de SI qualificada
- Estabelecer diretrizes e regras de SI adequadas e eficazes
- Caminhar junto!
- “Conviver” em segurança com dispositivos móveis e IoT

Desafios

FORUMRNP 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

- Usuários conscientes (em todos os campi!)
- Segurança além da tecnologia – processos implantados
- Conformidade com políticas, leis e marcos regulatórios e atendimento às auditorias
- Avançar a maturidade em SI em um cenário de restrição financeira
- Inserir o tema de forma rotineira na agenda da Alta Gestão

TCU

Estratégia para desenvolver a segurança da informação

E como a RNP pode ajudar?

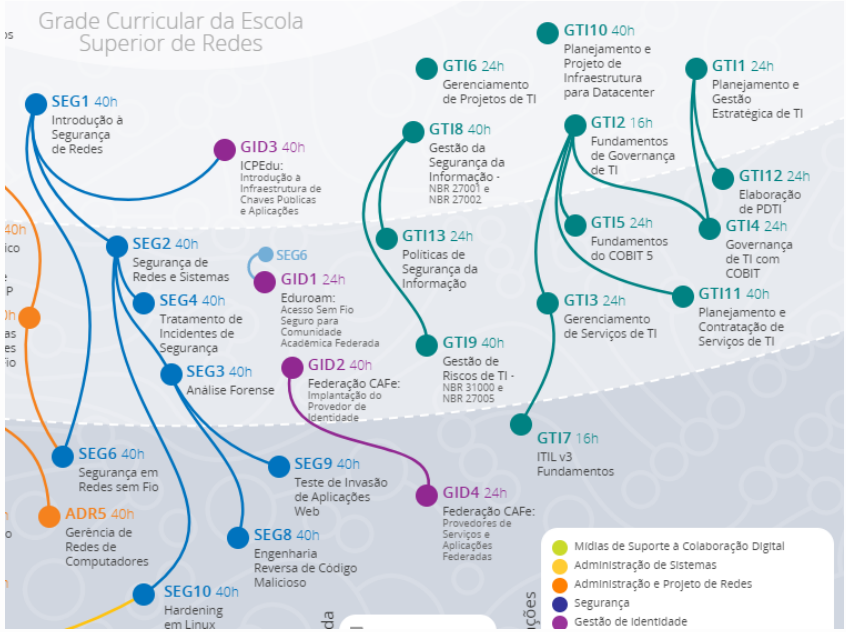
Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

- Gestor de segurança da informação
- Equipe qualificada



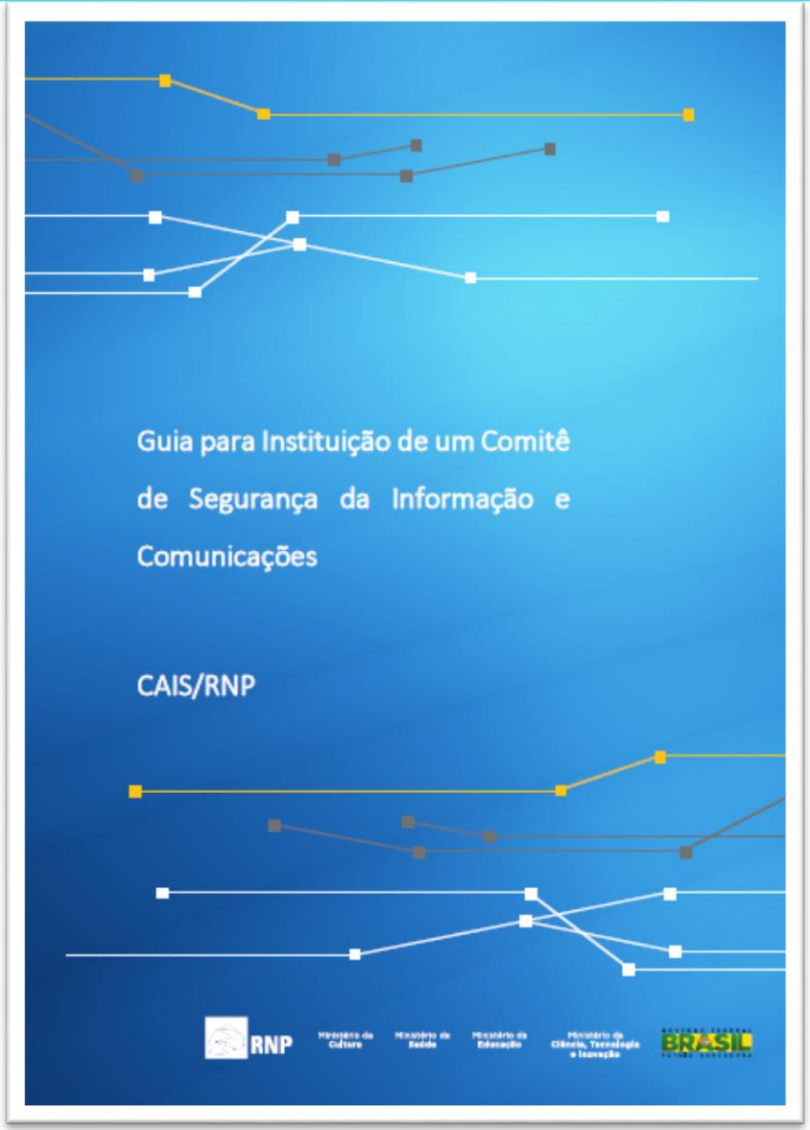
Escola Superior de Redes RNP

http://esr.rnp.br

Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

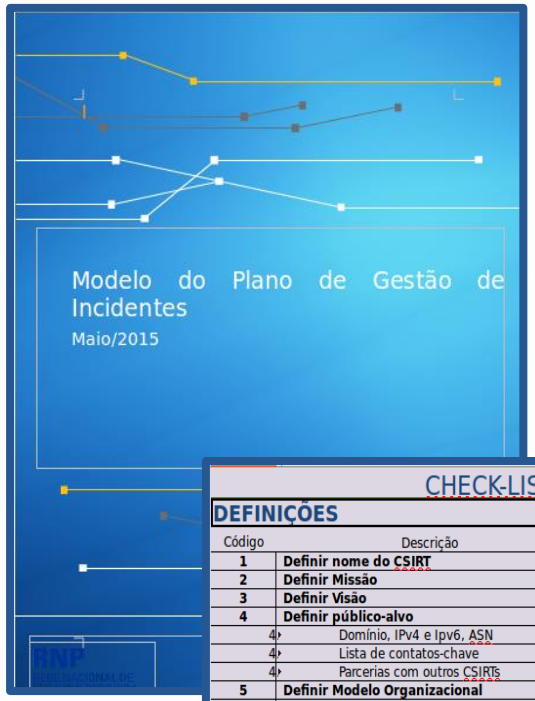
- CSIC

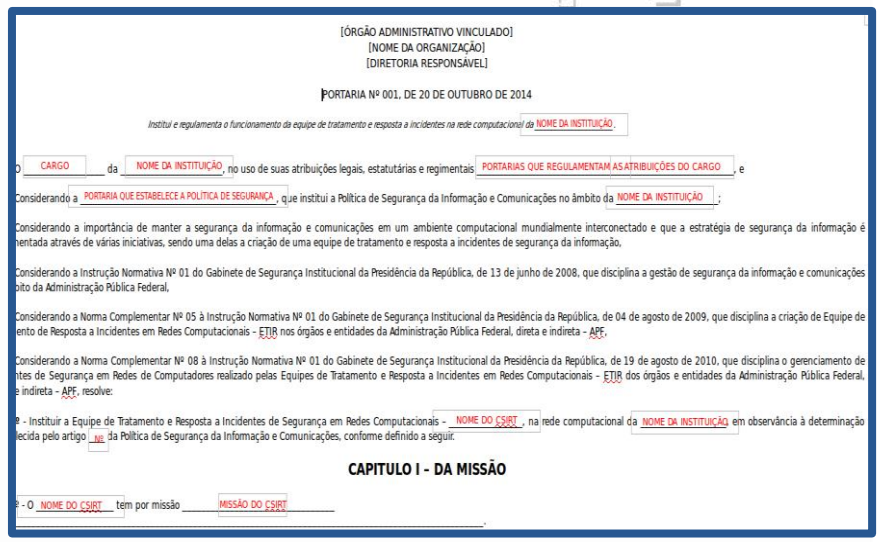


Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

- CSIRT





[ÓRGÃO ADMINISTRATIVO VINCULADO]
[NOME DA ORGANIZAÇÃO]
[DIRETORIA RESPONSÁVEL]

PORTARIA Nº 001, DE 20 DE OUTUBRO DE 2014

Institui e regulamenta o funcionamento da equipe de tratamento e resposta a incidentes na rede computacional da NOME DA INSTITUIÇÃO.

O CARGO da NOME DA INSTITUIÇÃO, no uso de suas atribuições legais, estatutárias e regimentais PORTARIAS QUE REGULAMENTAM AS ATRIBUIÇÕES DO CARGO, e

Considerando a PORTARIA QUE ESTABELECE A POLÍTICA DE SEGURANÇA, que institui a Política de Segurança da Informação e Comunicações no âmbito da NOME DA INSTITUIÇÃO;

Considerando a importância de manter a segurança da informação e comunicações em um ambiente computacional mundialmente interconectado e que a estratégia de segurança da informação é mentada através de várias iniciativas, sendo uma delas a criação de uma equipe de tratamento e resposta a incidentes de segurança da informação,

Considerando a Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações bito da Administração Pública Federal,

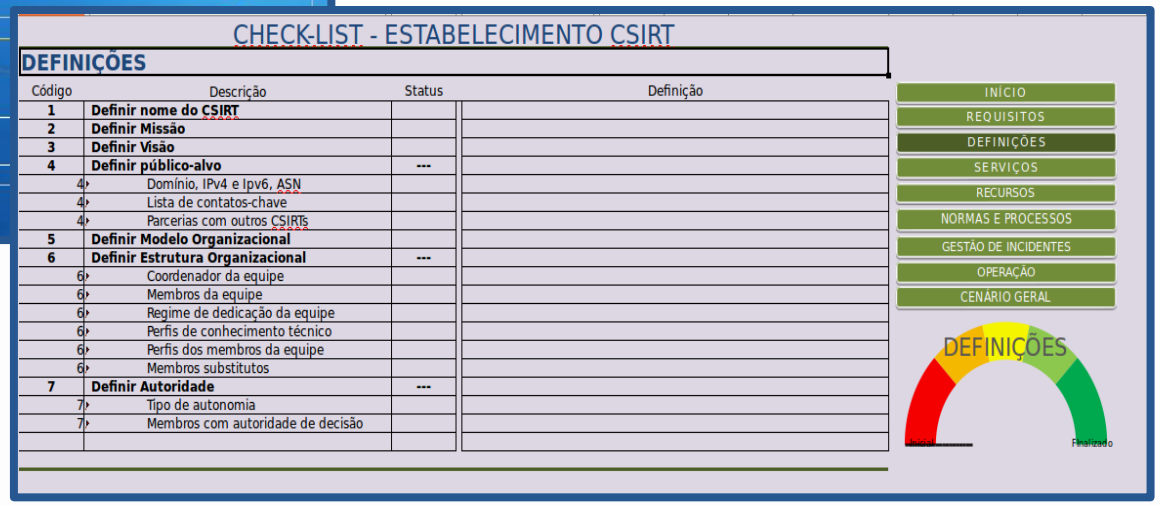
Considerando a Norma Complementar Nº 05 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 04 de agosto de 2009, que disciplina a criação de Equipe de ento de Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF,

Considerando a Norma Complementar Nº 08 à Instrução Normativa Nº 01 do Gabinete de Segurança Institucional da Presidência da República, de 19 de agosto de 2010, que disciplina o gerenciamento de ntes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, e indireta - APF, resolve:

º - Instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - NOME DO CSIRT, na rede computacional da NOME DA INSTITUIÇÃO em observância à determinação lecida pelo artigo nº da Política de Segurança da Informação e Comunicações, conforme definido a seguir.

CAPITULO I - DA MISSÃO

º - O NOME DO CSIRT tem por missão MISSÃO DO CSIRT.



CHECK-LIST - ESTABELECIMENTO CSIRT

DEFINIÇÕES

Código	Descrição	Status	Definição
1	**Definir nome do CSIRT**		
2	**Definir Missão**		
3	**Definir Visão**		
4	**Definir público-alvo**	---	
4›	Domínio, IPv4 e Ipv6, ASN		
4›	Lista de contatos-chave		
4›	Parcerias com outros CSIRTs		
5	**Definir Modelo Organizacional**		
6	**Definir Estrutura Organizacional**	---	
6›	Coordenador da equipe		
6›	Membros da equipe		
6›	Regime de dedicação da equipe		
6›	Perfis de conhecimento técnico		
6›	Perfis dos membros da equipe		
6›	Membros substitutos		
7	**Definir Autoridade**	---	
7›	Tipo de autonomia		
7›	Membros com autoridade de decisão		

INÍCIO
REQUISITOS
DEFINIÇÕES
SERVIÇOS
RECURSOS
NORMAS E PROCESSOS
GESTÃO DE INCIDENTES
OPERAÇÃO
CENÁRIO GERAL

DEFINIÇÕES

Comprometimento da Alta Gestão

↓

Definição e atribuição de papéis relacionados à SI

↓

Diagnóstico do status atual da SI

Comprometimento da Alta Gestão

↓

Definição e atribuição de papéis relacionados à SI

↓

Diagnóstico do status atual da SI

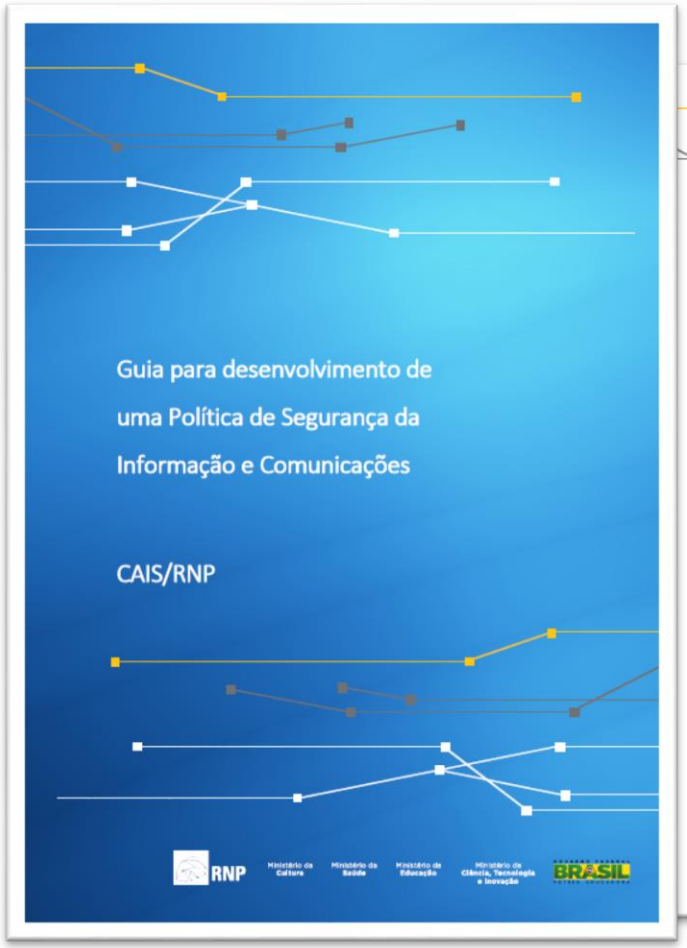
↓

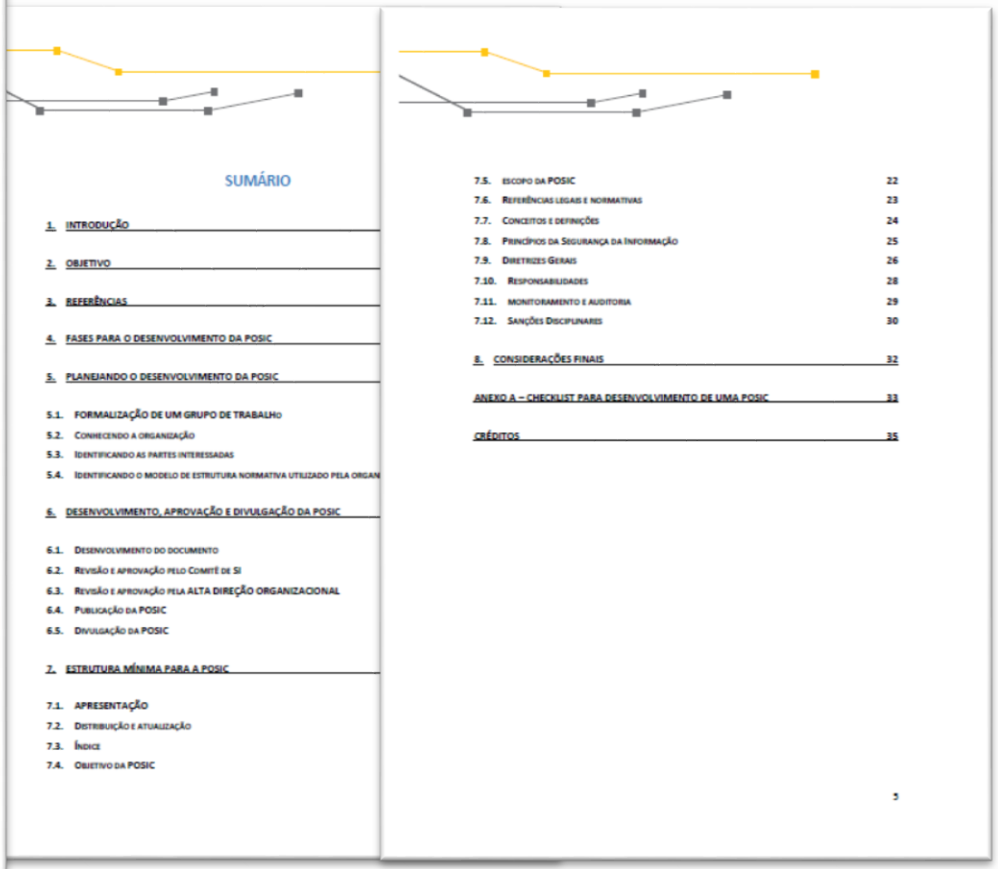
Elaboração e aprovação da POSIC

Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

Elaboração e aprovação da POSIC





SUMÁRIO

Comprometimento da Alta Gestão

↓

Definição e atribuição de papéis relacionados à segurança

↓

Elaboração e aprovação da POSIC

↓

Implantação de processos

Envolvimento e comprometimento da Alta Gesto

Definição e atribuição de papéis relacionados à segurança

Elaboração e aprovação da POSIC

Implantação de processos

Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

Elaboração e aprovação da POSIC

Implantação de processos

Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

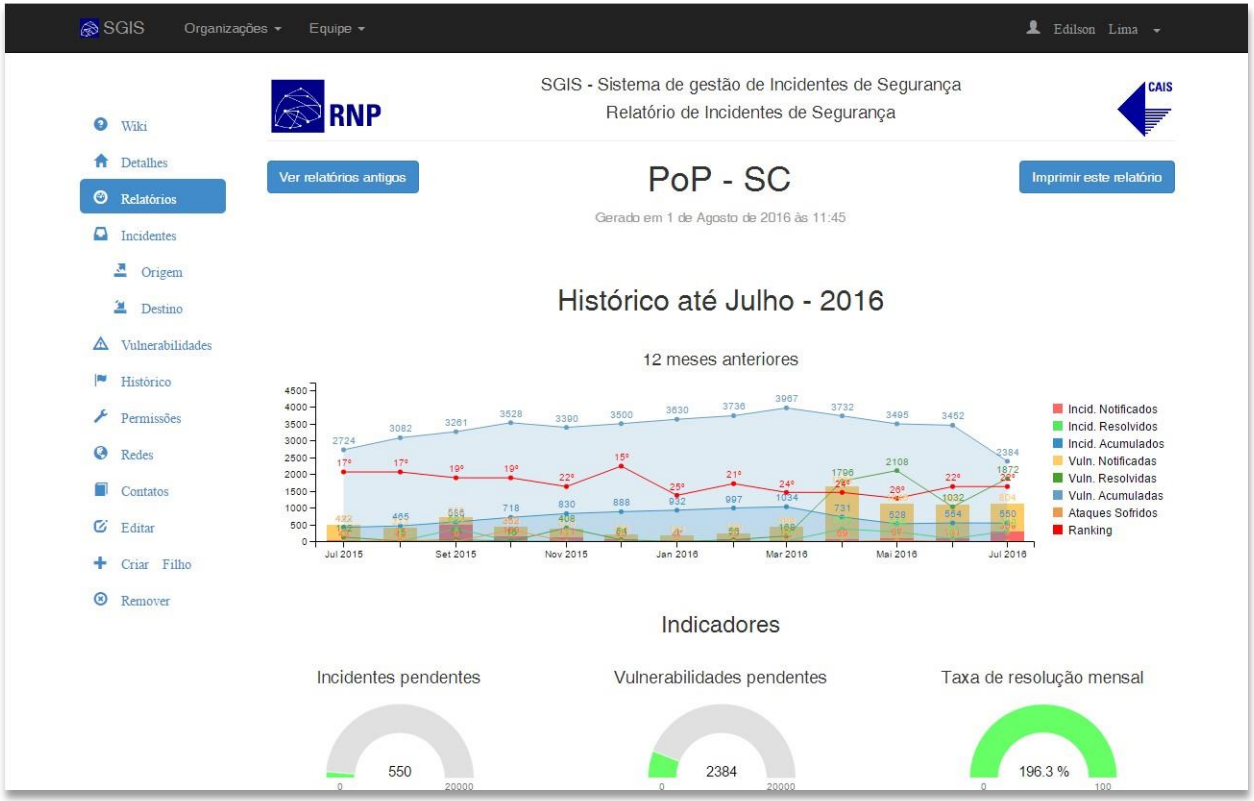
Elaboração e aprovação da POSIC

Implantação de processos

Sistema para gestão de incidentes e vulnerabilidades de segurança.

Consolidador de todas as vulnerabilidades e incidentes.

Mais de 1.400 usuários ativos (técnicos e gestores)

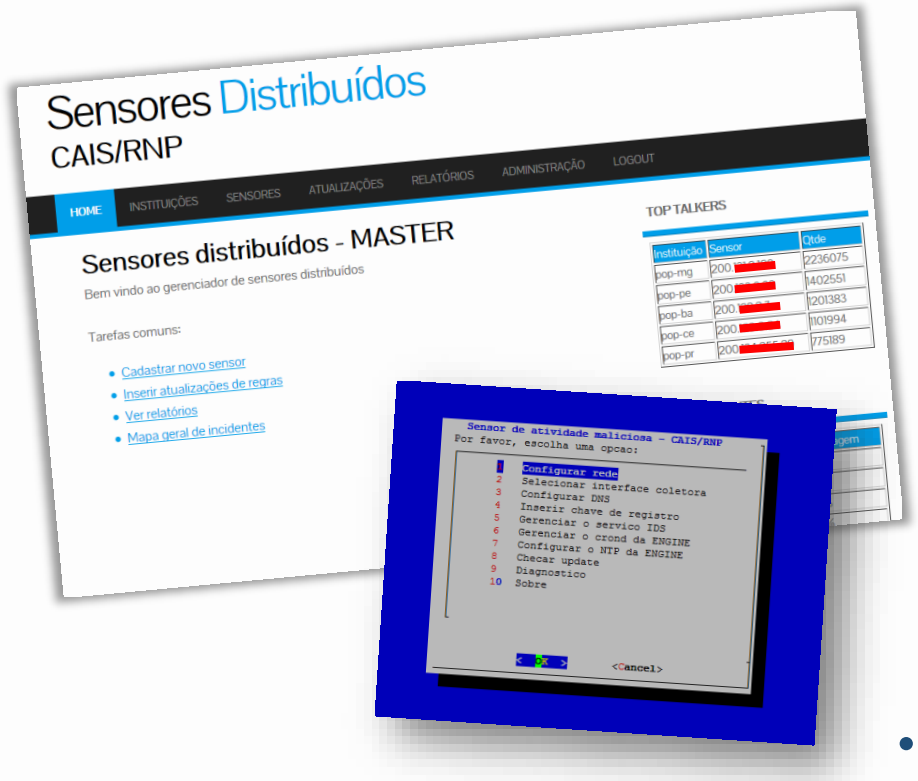


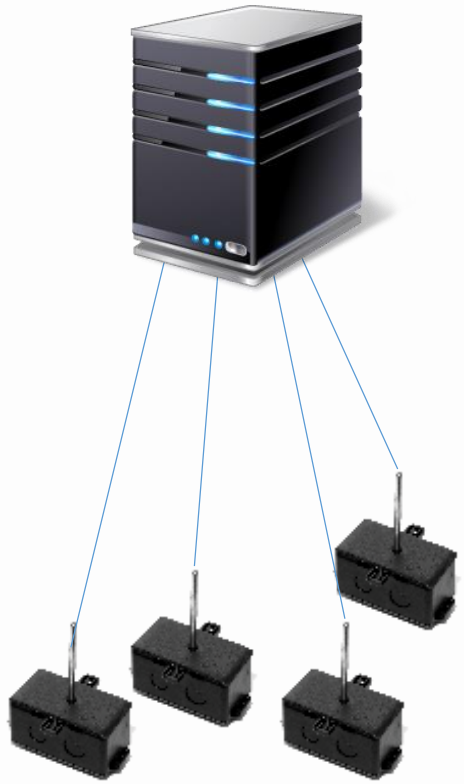
Envolvimento e comprometimento da Alta Gestão

Definição e atribuição de papéis relacionados à segurança

Elaboração e aprovação da POSIC

Implantação de processos





- 44 sensores ativos (27 PoPs + 17 clientes)
- ~ 1.000 detecções x sensor x dia

Comprometimento da Alta Gestão

↓

Definição e atribuição de papéis relacionados à SI

↓

Diagnóstico da situação atual da SI

↓

Elaboração e aprovação da POSIC

↓

Implantação de processos

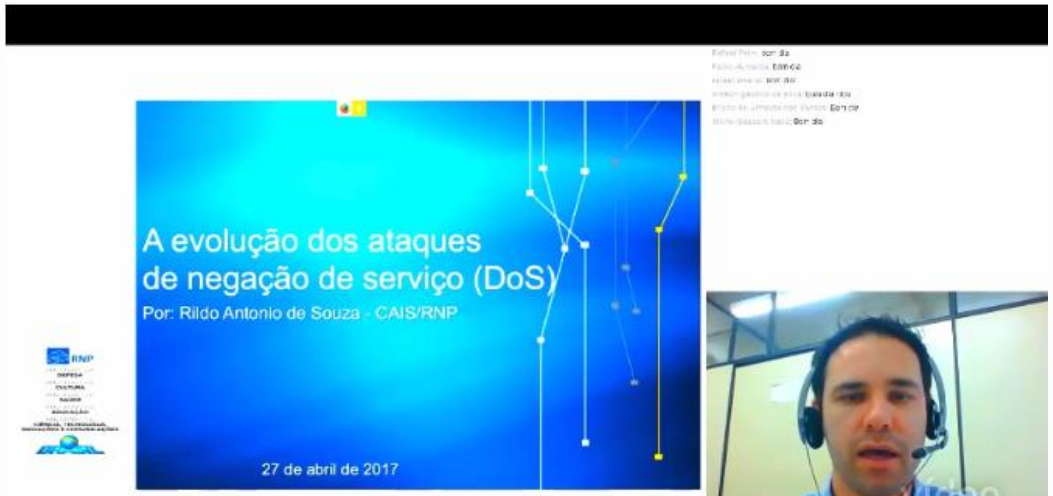
↓

Conscientização e treinamento

- Envolvimento e comprometimento da Alta Gestão
- Definição e atribuição de papéis relacionados à segurança
- Elaboração e aprovação da POSIC
- Implantação de processos
- **Conscientização e treinamento**

- Envolvimento e comprometimento da Alta Gestão
- Definição e atribuição de papéis relacionados à segurança
- Elaboração e aprovação da POSIC
- Implantação de processos
- **Conscientização e treinamento**

Webinar - A evolução dos ataques de DoS



Webinar - Backup - O básico cada vez mais essencial

- Envolvimento e comprometimento da Alta Gestão
- Definição e atribuição de papéis relacionados à segurança
- Elaboração e aprovação da POSIC
- Implantação de processos
- **Conscientização e treinamento**

Melhoria contínua e conformidade

Segurança da informação nos campi: desafios e tendências

Ou provocações para o debate!

Quebrar o paradigma atual: segurança não é apenas apagar incêndio!

Liberdade e privacidade do usuário como direito garantido. Como conciliar com as necessidades de proteção da informação?

Investir mais em tecnologia e processos. Depender menos do usuário.

Segurança além de servidores e estações: os velhos problemas retornam agora com dispositivos móveis e IoT.

Migração segura para Nuvem e em conformidade com a legislação

Atuação em rede para o fortalecimento da segurança.

Obrigada!

Carla Freitas

Carla.Freitas@rnp.br