



FÓRUM RNP 2017

25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

Segurança da informação nos campi: desafios e tendências

Carla Freitas - RNP



Segurança da informação nos campi: desafios e tendências



Cenário da TIC nos campi

Cenário da TIC nos campi

FÓRUM **RNP** 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS



Equipe reduzida



Recursos limitados



Várias TIC dentro da
organização

Cenário de TIC nos campi

FÓRUM **RNP** 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS



Grande número de usuários com alta rotatividade



Alto uso de dispositivos móveis



Grande quantidade de computadores

Cenário de TIC nos campi

FÓRUM **RNP** 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS



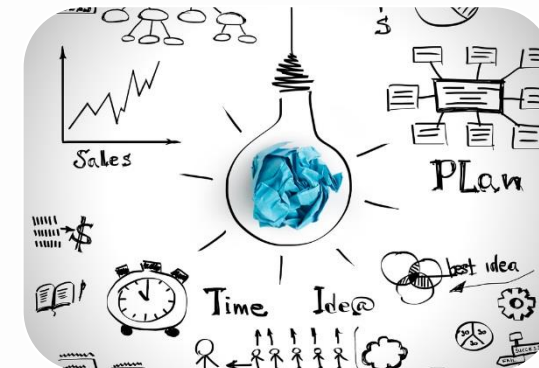
Diversos softwares e sistemas



Rede com alta capacidade e disponibilidade



Diferentes perfis (visitante, acadêmico e administrativo)



Necessidade de “liberdade” para a pesquisa

Cenário de TIC nos campi

FÓRUM RNP 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 ;)

190192037.mvfrebsites.net

Bem-vindo ao Horde (mantido pela ...)

De Universidade de actualização Email Conta <helpdesk@...> ☆
Assunto **Universidade de actualização Email Conta**
Para

Username

Password

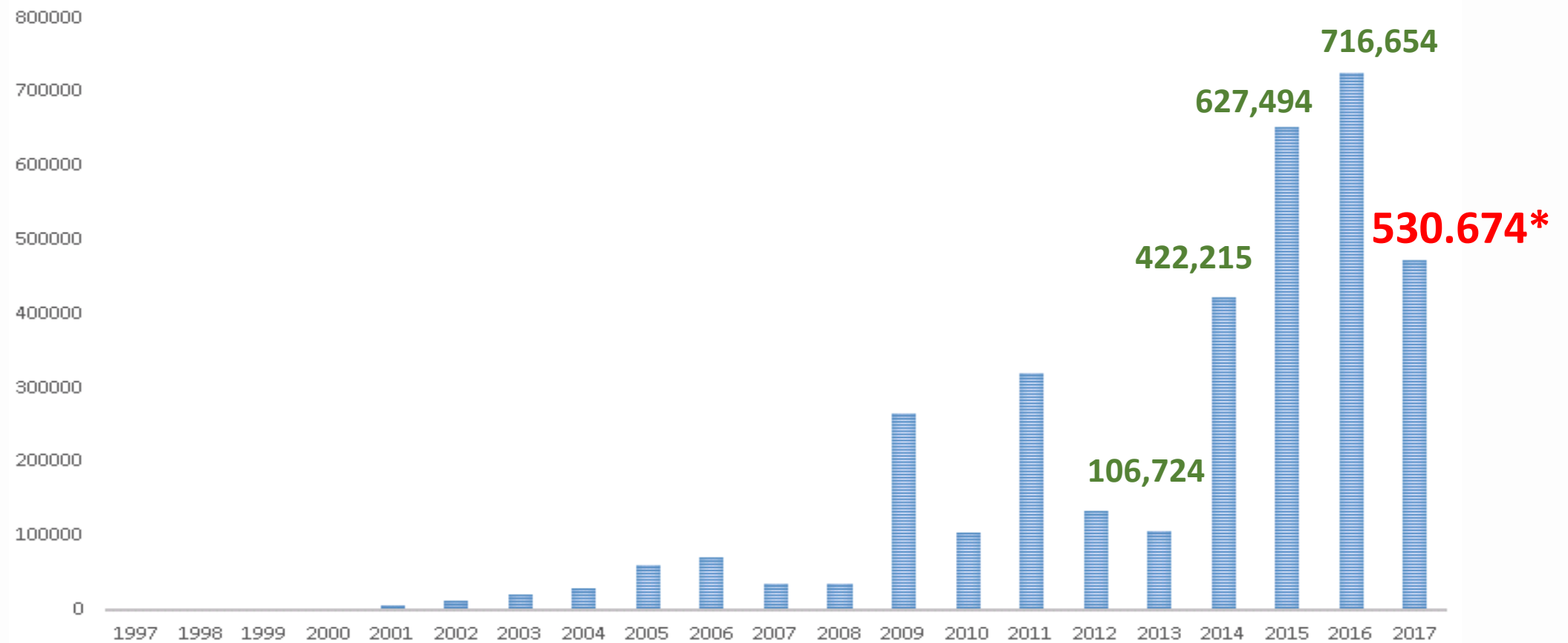
Log In

--
Atenção
Estamos actualmente a fazer o processo de manutenção de todos os e-mails imediatamente a este e-mail, para verificar sua conta contra spyware seguindo os links.
Para atualizar, clique aqui
<http://190192037.mvfrebsites.net/>

SiteBuilder.com

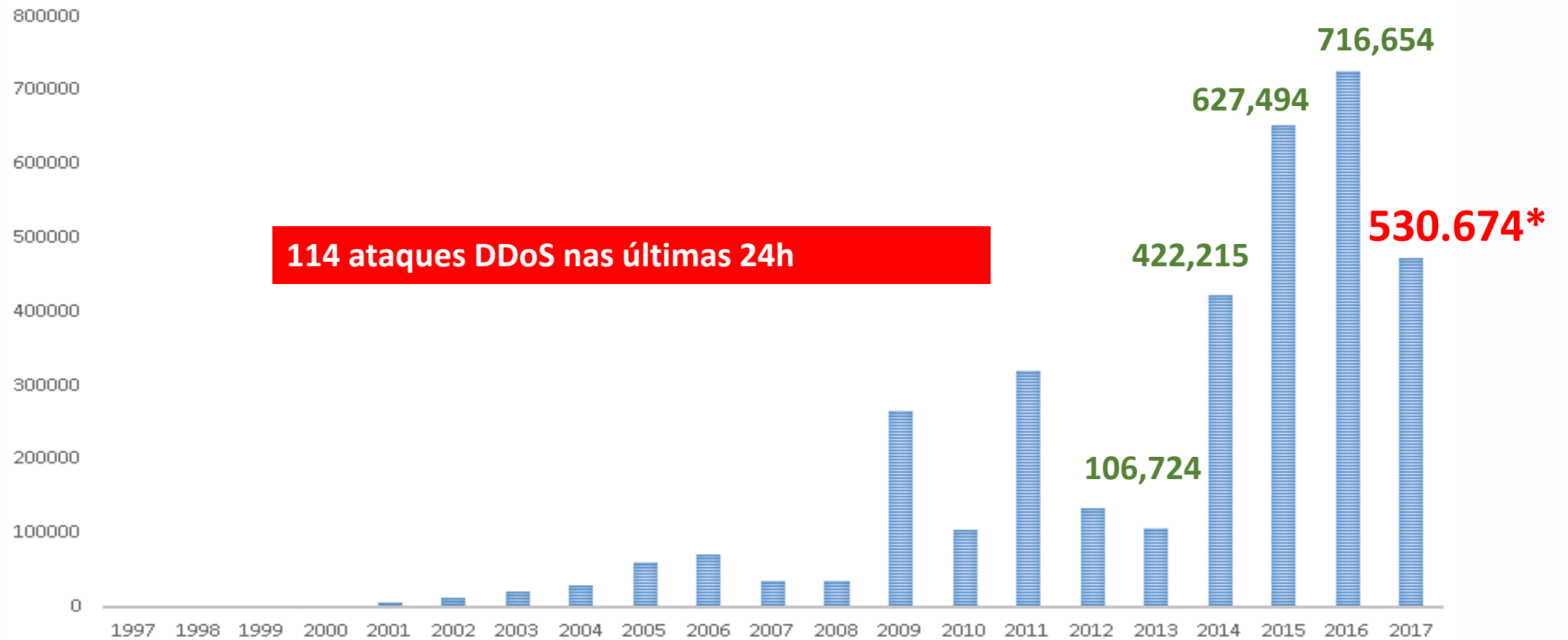
Built using SiteBuilder. Create your FREE website today!

Alvo de ataque: visibilidade, questão política e ambiente propício



*Até Set/2017

Alvo de ataque: visibilidade, questão política e ambiente propício

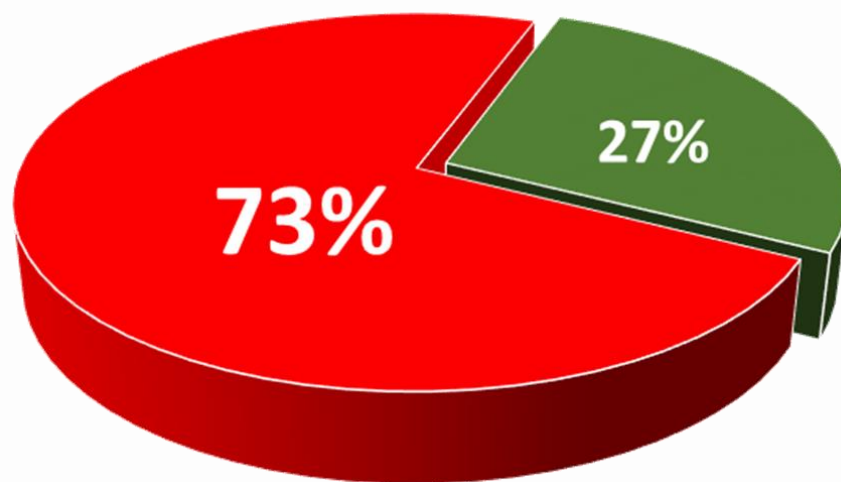


* Até Set/2017

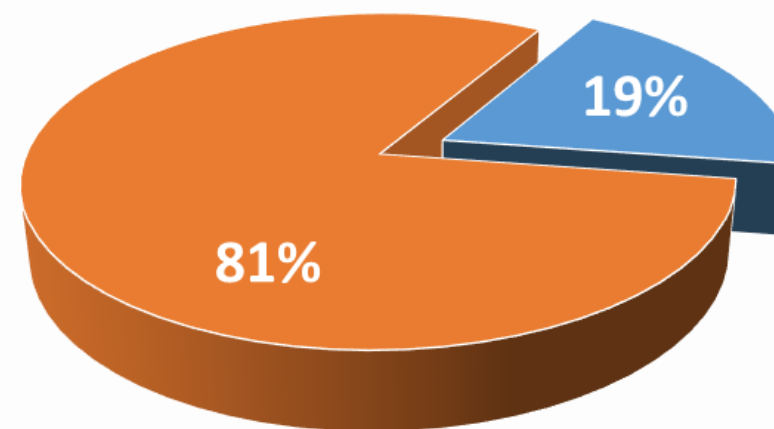
Cenário de TIC nos campi

FÓRUM RNP 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

Alvo de ataque: visibilidade, questão política e ambiente propício



■ Notificações de incidentes respondidas
■ Incidentes sem resposta



■ Notificações de vulnerabilidades respondidas
■ Vulnerabilidades sem tratamento

*Período: Set/2016 a Set/2017

86,4% dos incidentes tem como origem um cliente

Segurança da informação nos campi: **desafios** e tendências

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

FÓRUM RNP 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



Segurança da informação nos campi: desafios e tendências



FÓRUM **RNP** 2017
25 ANOS DE INTERNET NO BRASIL
DESAFIOS E TENDÊNCIAS

Estratégia para desenvolver a segurança da informação

E como a RNP pode ajudar?

Envolvimento e
comprometimento da
Alta Gestão

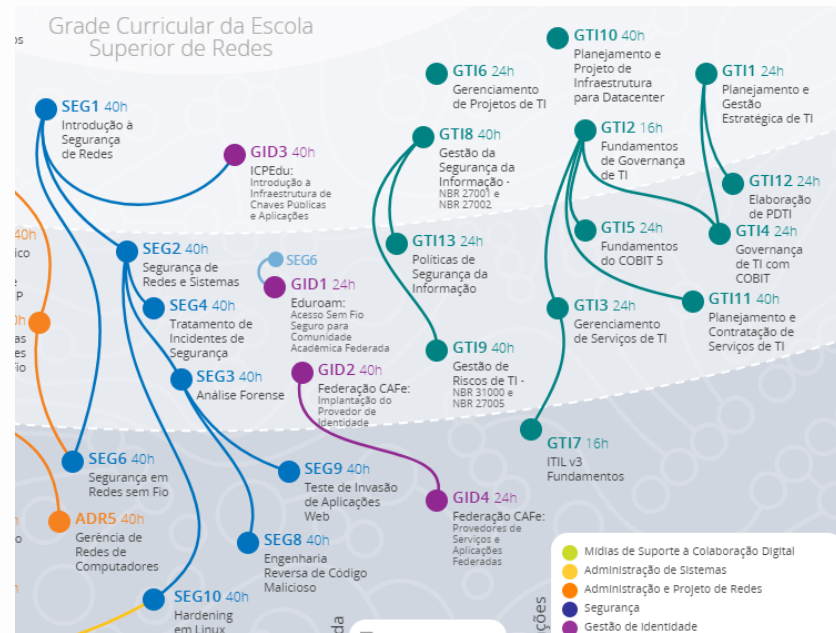


Definição e atribuição
de papéis
relacionados à
segurança

Envolvimento e
comprometimento
da Alta Gestão

- Gestor de segurança da informação
- Equipe qualificada

Definição e
atribuição de papéis
relacionados à
segurança



<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

- CSIRT

Definição e
atribuição de papéis
relacionados à
segurança



[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 adotada 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 no âmbito 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 Tratamento e 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 Redes 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, direta e indireta - [APF], resolve:

1º - 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 contida no artigo [Nº] da Política de Segurança da Informação e Comunicações, conforme definido a seguir:

CAPÍTULO I - DA MISSÃO

1º - O [NOME DO CSIRT] tem por missão [MISSÃO DO CSIRT].

CHECK-LIST - ESTABELECIMENTO CSIRT

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

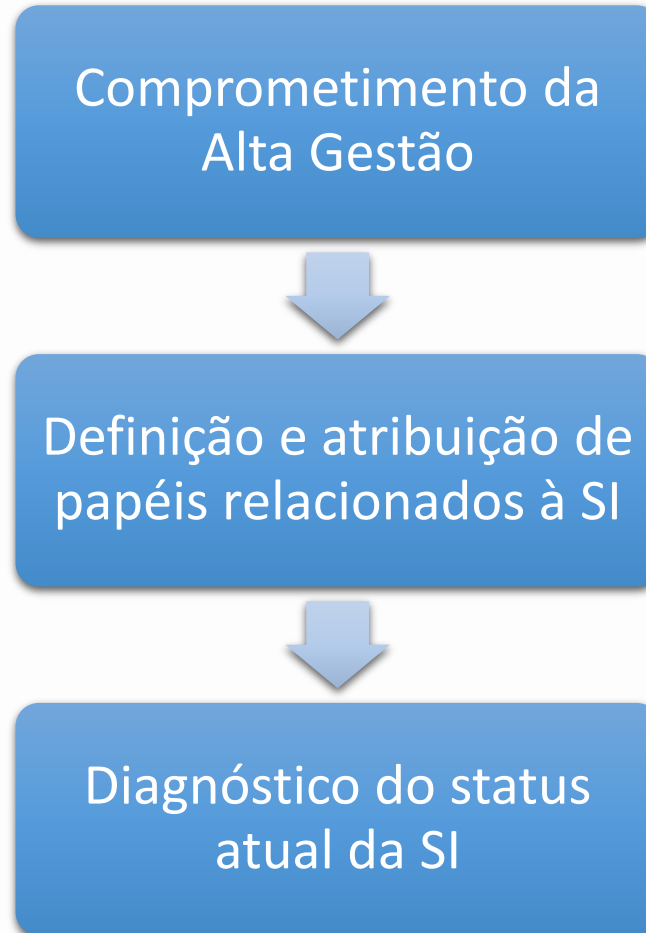
RECURSOS

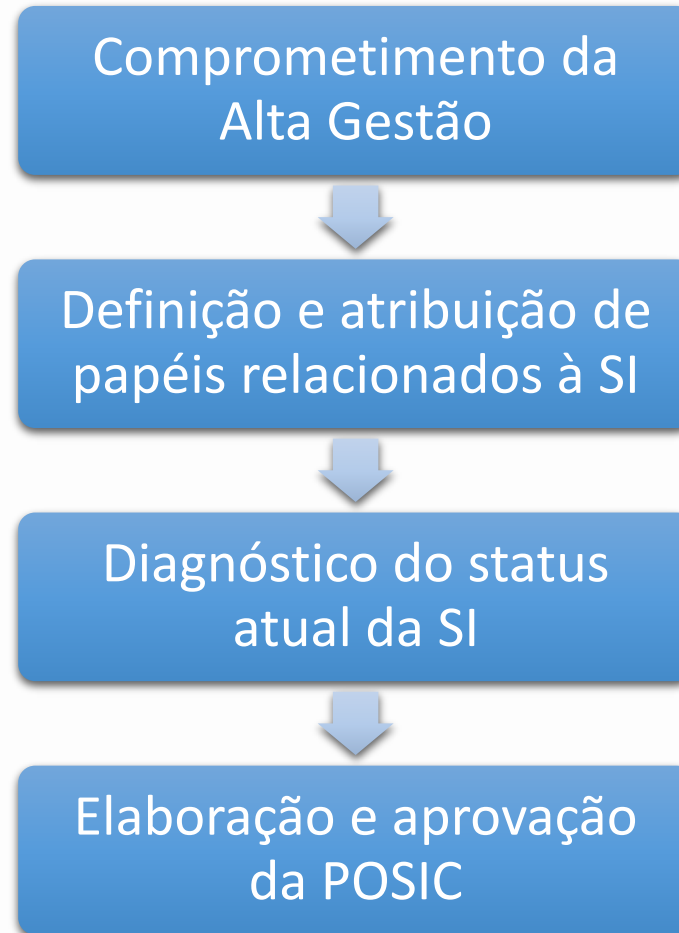
NORMAS E PROCESSOS

GESTÃO DE INCIDENTES

OPERAÇÃO

CENÁRIO GERAL





Envolvimento e
comprometimento da
Alta Gestão



Definição e atribuição
de papéis relacionados
à segurança



Elaboração e
aprovação da POSIC



SUMÁRIO	
1. INTRODUÇÃO	
2. OBJETIVO	
3. REFERÊNCIAS	
4. FASES PARA O DESENVOLVIMENTO DA POSIC	
5. PLANEJANDO O DESENVOLVIMENTO DA POSIC	
5.1. FORMALIZAÇÃO DE UM GRUPO DE TRABALHO	
5.2. CONHECENDO A ORGANIZAÇÃO	
5.3. IDENTIFICANDO AS PARTES INTERESSADAS	
5.4. IDENTIFICANDO O MODELO DE ESTRUTURA NORMATIVA UTILIZADO PELA ORGANIZAÇÃO	
6. DESENVOLVIMENTO, APROVAÇÃO E DIVULGAÇÃO DA POSIC	
6.1. DESENVOLVIMENTO DO DOCUMENTO	
6.2. REVISÃO E APROVAÇÃO PELO COMITÊ DE SI	
6.3. REVISÃO E APROVAÇÃO PELA ALTA DIREÇÃO ORGANIZACIONAL	
6.4. PUBLICAÇÃO DA POSIC	
6.5. DIVULGAÇÃO DA POSIC	
7. ESTRUTURA MÍNIMA PARA A POSIC	
7.1. APRESENTAÇÃO	
7.2. DISTRIBUIÇÃO E ATUALIZAÇÃO	
7.3. ÍNDICE	
7.4. OBJETIVO DA POSIC	
7.5. ESCOPO DA POSIC	22
7.6. REFERÊNCIAS LEGAIS E NORMATIVAS	23
7.7. CONCEITOS E DEFINIÇÕES	24
7.8. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO	25
7.9. DIRETRIZES GERAIS	26
7.10. RESPONSABILIDADES	28
7.11. MONITORAMENTO E AUDITORIA	29
7.12. SANÇÕES DISCIPLINARES	30
8. CONSIDERAÇÕES FINAIS	32
ANEXO A – CHECKLIST PARA DESENVOLVIMENTO DE UMA POSIC	33
CRÉDITOS	35

Comprometimento da Alta
Gestão



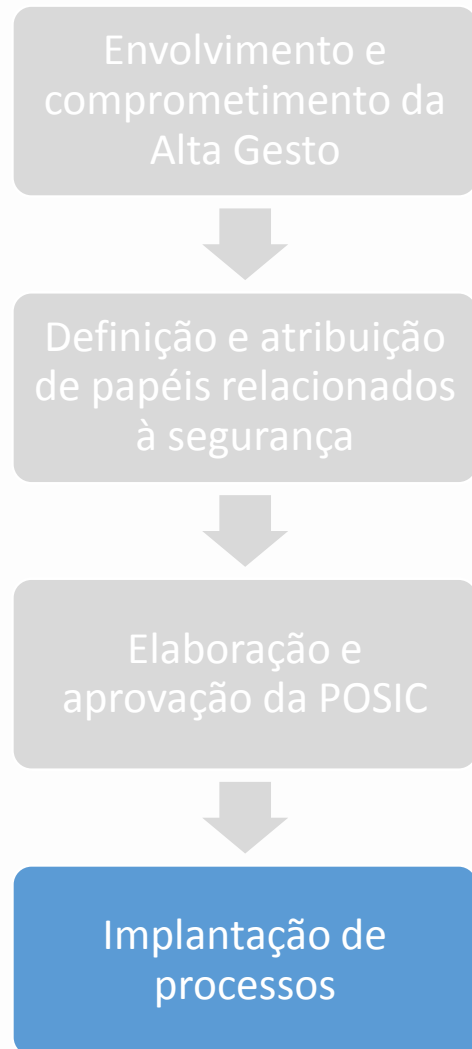
Definição e atribuição de
papéis relacionados à
segurança

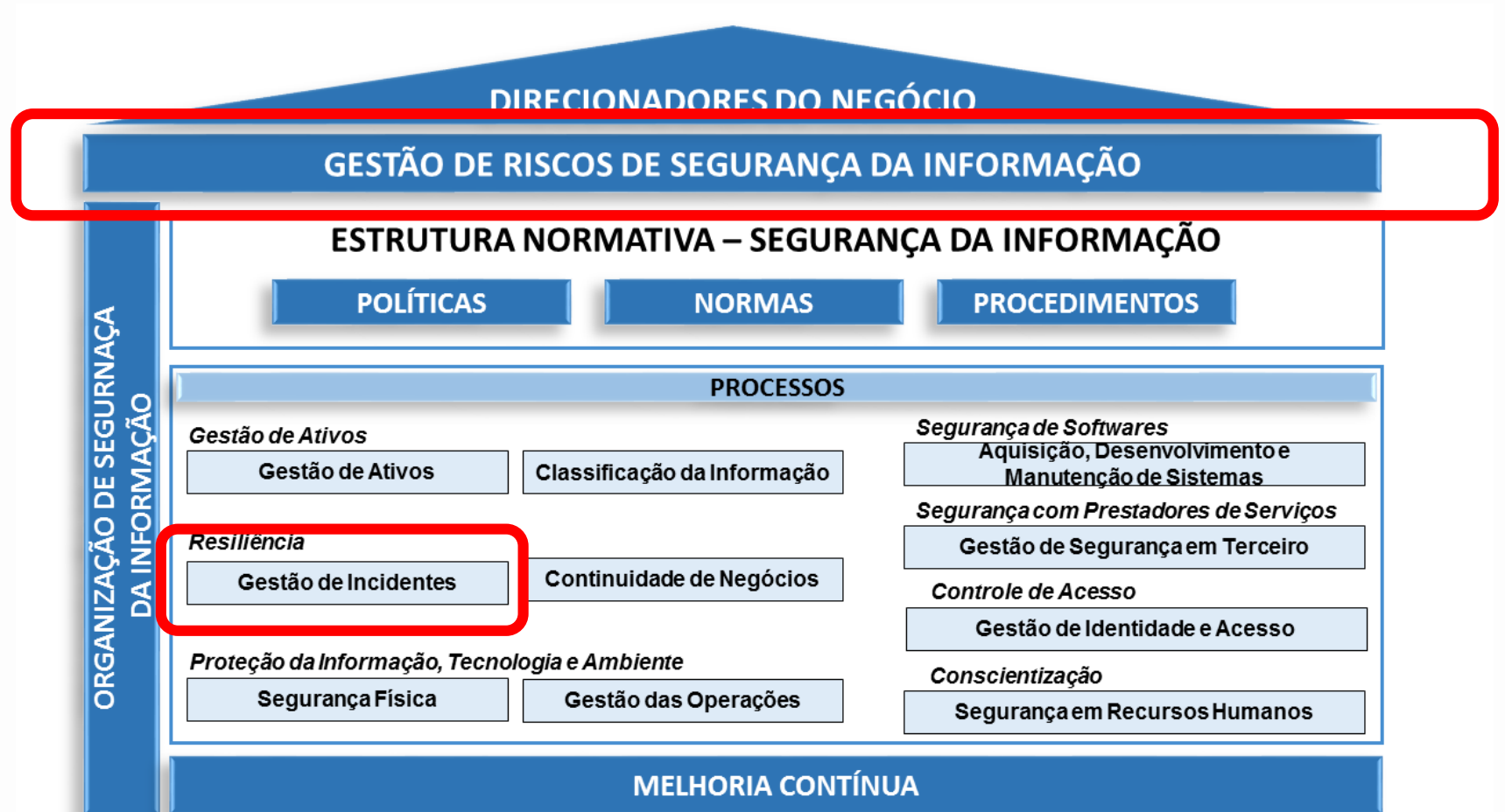
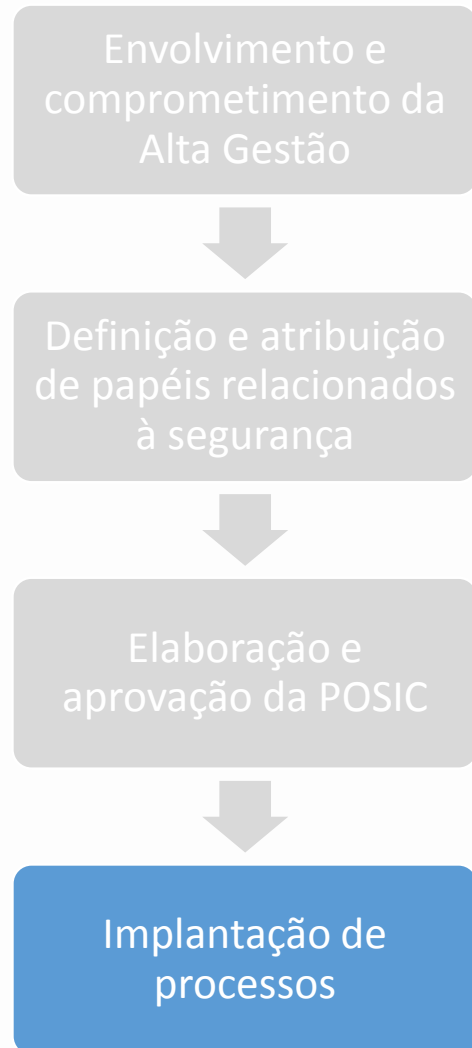


Elaboração e aprovação da
POSIC



Implantação de processos





Envolvimento e comprometimento da Alta Gestão



Definição e atribuição de papéis relacionados à segurança



Elaboração e aprovação da POSIC

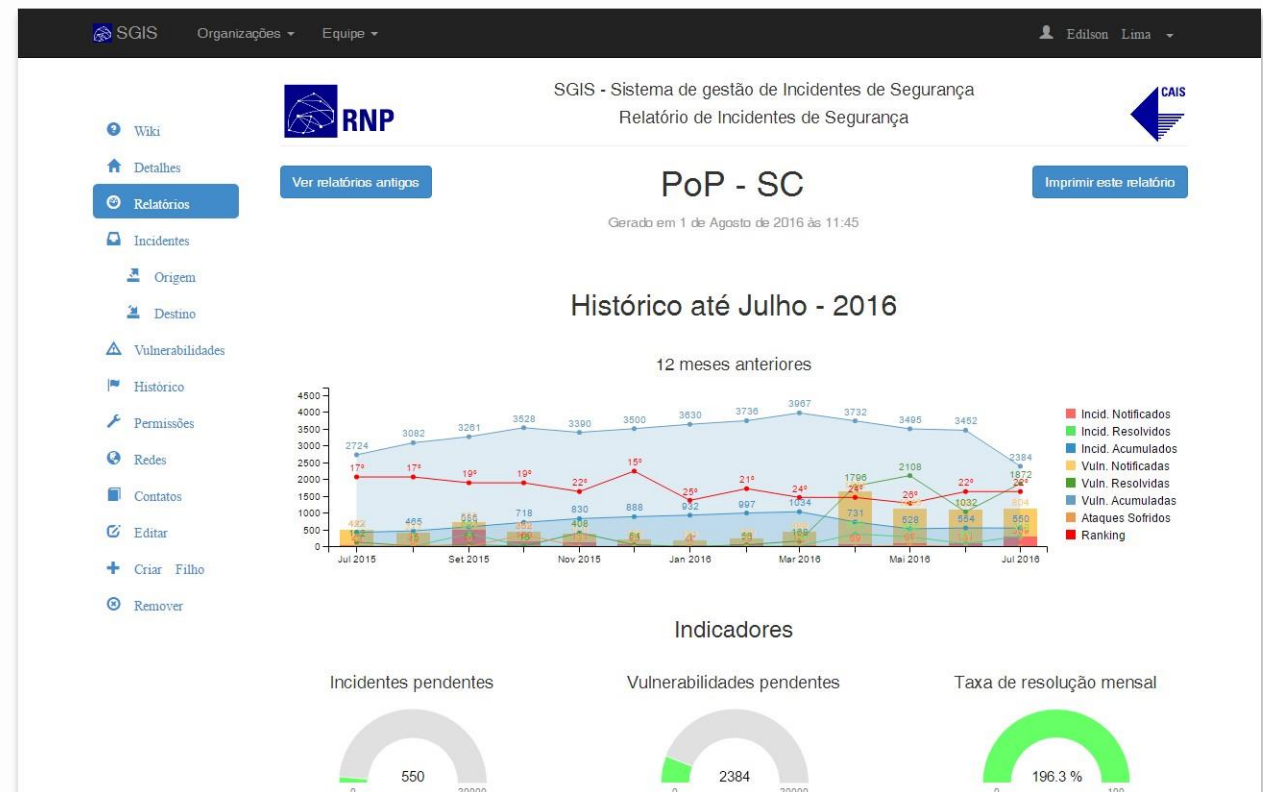


Implantação de processos

Sistema para gestão de incidentes e vulnerabilidades de segurança.

Mais de 1.400 usuários ativos (técnicos e gestores)

Consolidador de todas as vulnerabilidades e incidentes.



Envolvimento e comprometimento da Alta Gestão



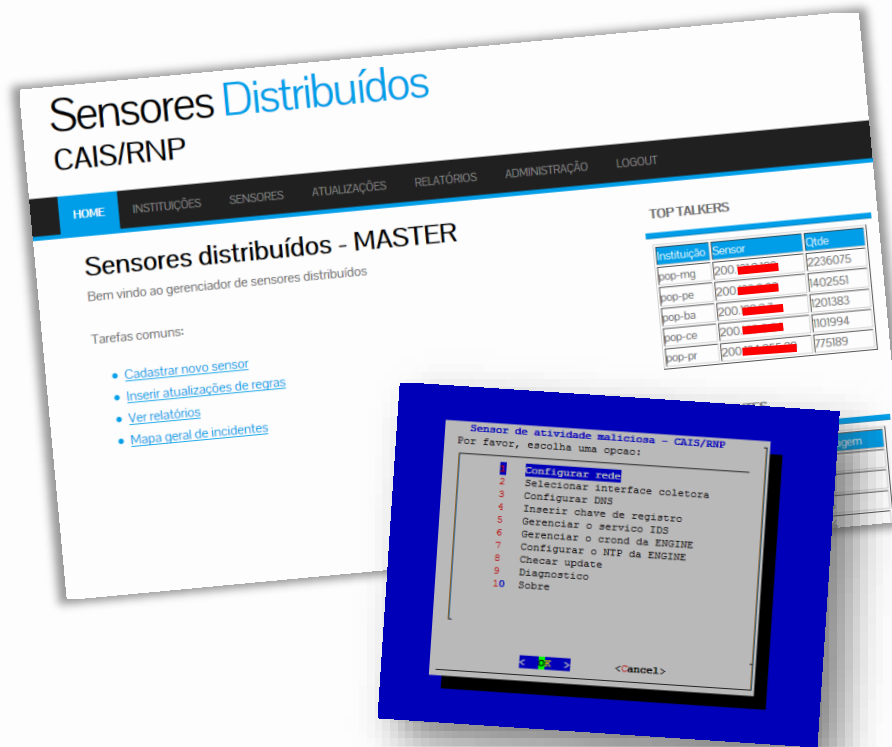
Definição e atribuição de papéis relacionados à segurança



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



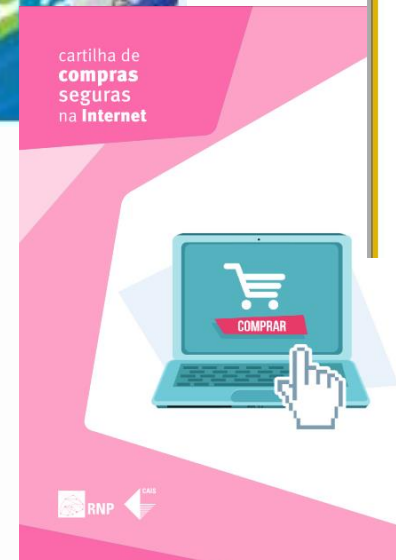
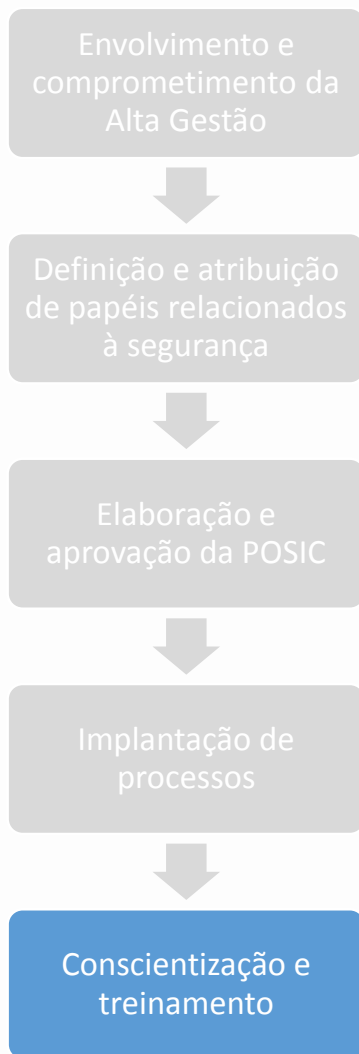
Elaboração e aprovação da
POSIC



Implantação de processos



Conscientização e
treinamento



CAIS RESUMO 1º SEM17 N.6 Alertas, vulnerabilidades e incidentes de segurança Ransomwares causam uma das maiores crises cibernéticas a nível mundial Ransomware é um tipo de malware que se utiliza do recurso da criptografia para bloquear acesso de um usuário a arquivos e sistemas de seu computador e/ou dispositivo móvel, os quais são (ou, pelo menos, tem a promessa de serem) liberados somente mediante pagamento de resgate. Apesar de estarem atualmente com frequência nas manchetes de jornais e televisões, esta não é uma ameaça recente. O primeiro malware com as mesmas características dos ransomwares que conhecemos atualmente foi desenvolvido em 1989. De lá para cá, a sofisticação do uso malicioso da criptografia tem cada vez mais comprometido computadores e sistemas, afetando usuários, serviços e economias ao redor do mundo. Somente em 2016, foram descobertas quase 200 novas famílias de ransomwares e o número de novas variantes cresceram cerca de 600%. O CAIS também destacou os riscos e a tendência ao aumento desse tipo de ataque na versão do CAIS EM RESUMO N.5, que foi publicado em setembro de 2015. Na época, vários especialistas já alertavam a comunidade para as medidas preventivas necessárias a serem adotadas por administradores de redes, equipes de segurança e usuários em geral. Os mais recentes casos de ransomware, conhecidos como WannaCry, ou WannaCryptor, e o NotPetya causaram grandes prejuízos no primeiro semestre de 2017, comprometendo milhares de computadores em mais de 150 países, incluindo o Brasil (figura 1). Foram registrados casos de infecção por esses ransomwares em órgãos do serviço público e também em instituições que fazem uso da rede brasileira de ensino e pesquisa. The 'Wannacry' ransomware attack The attack has hit more than 200,000 victims in at least 150 countries, says Europol Figura 1 Fonte: intel.malwarewatch.com	CAIS EM RESUMO é uma publicação periódica do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS/RNP), que tem como objetivo apresentar os principais acontecimentos relacionados à área de segurança da informação que impactaram a rede acadêmica e de pesquisa no último semestre, bem como as principais realizações do CAIS no período.
---	---

Webinar - A evolução dos ataques de DoS

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

A evolução dos ataques de negação de serviço (DoS)

Por: Rildo Antonio de Souza - CAIS/RNP

27 de abril de 2017



Webinar - Backup - O básico cada vez mais essencial

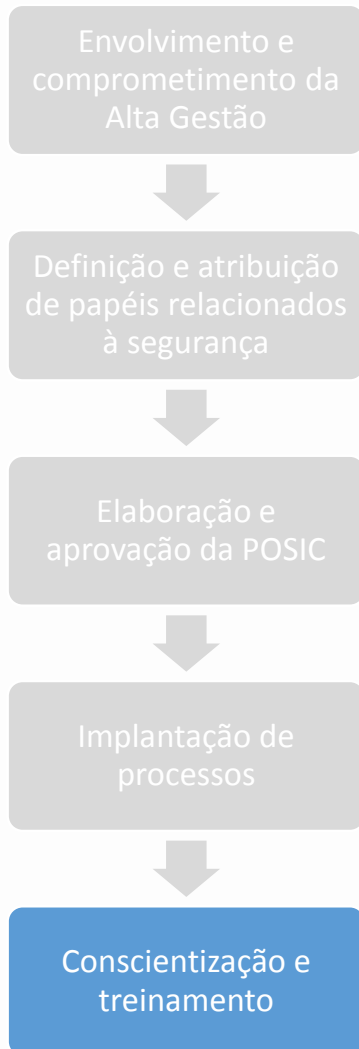
RNP (Gravando) Seminários de Segurança da Informação - CAIS/RNP

PFSI - Programa de Fomento à Segurança da Informação

Seminários online

Qual o valor dos dados

- Difícil mensurar
- Geralmente só é percebido da maneira mais difícil
- Dados:
 - possuem valor emocional, financeiro, acadêmico, jurídico, etc.
 - levam tempo ou são impossíveis de serem refeitos
- Perda pode afetar:
 - a continuidade dos negócios
 - perda de clientes/pacientes, downtime, etc
 - reputação/imagem da empresa
 - moral da equipe
- Como protegê-los?





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

