CSIRTs: como montar seu *Hackbusters*

GTS 28

VI Semana de Infraestrutura da Internet no Brasil

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

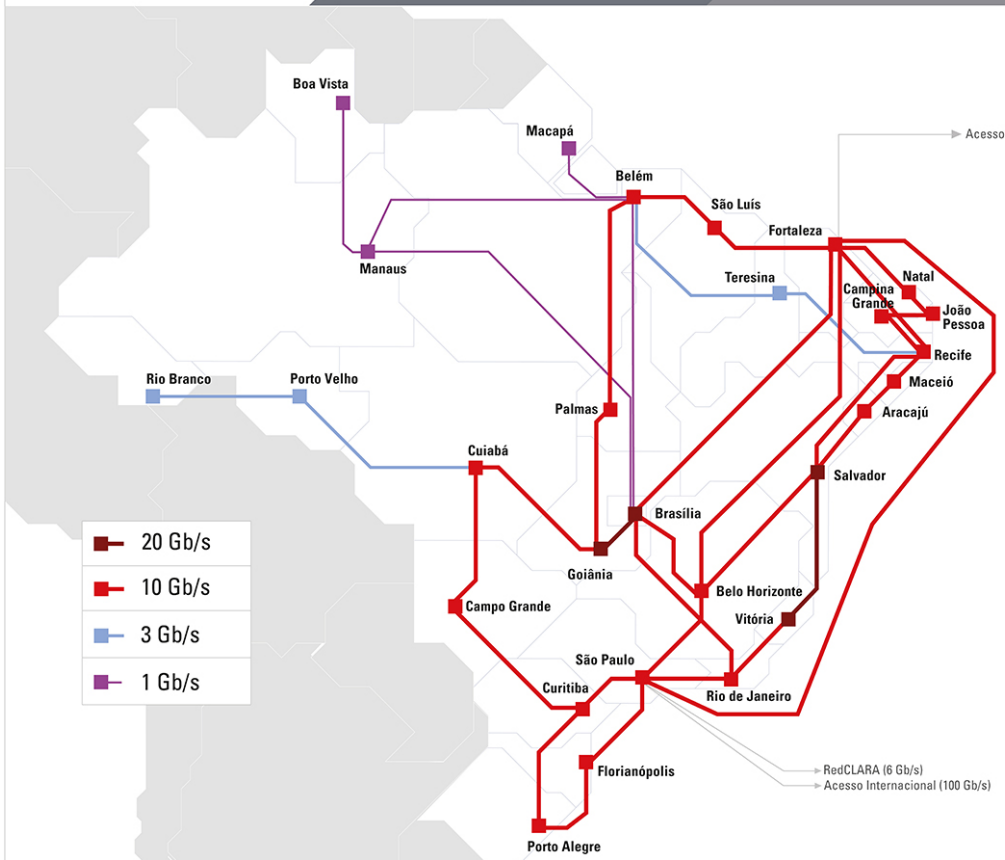
cgi.br Comitê Gestor da Internet no Brasil

nic.br Núcleo de Informação e Coordenação do Ponto BR

A RNP

Missão: promover o uso inovador de redes avançadas.

Conexão em 2016 | capacidade agregada 347 Gb/s | capacidade internacional 116 Gb/s



redeIpê

Comunidade de ensino e pesquisa:

- ✓ Escolas de educação superior;
- ✓ Universidades;
- ✓ Centros de Tecnologia;
- ✓ Laboratórios Nacionais;
- ✓ Institutos de pesquisa;
- ✓ Museus;
- ✓ Hospitais Universitários;
- ✓ Outros;

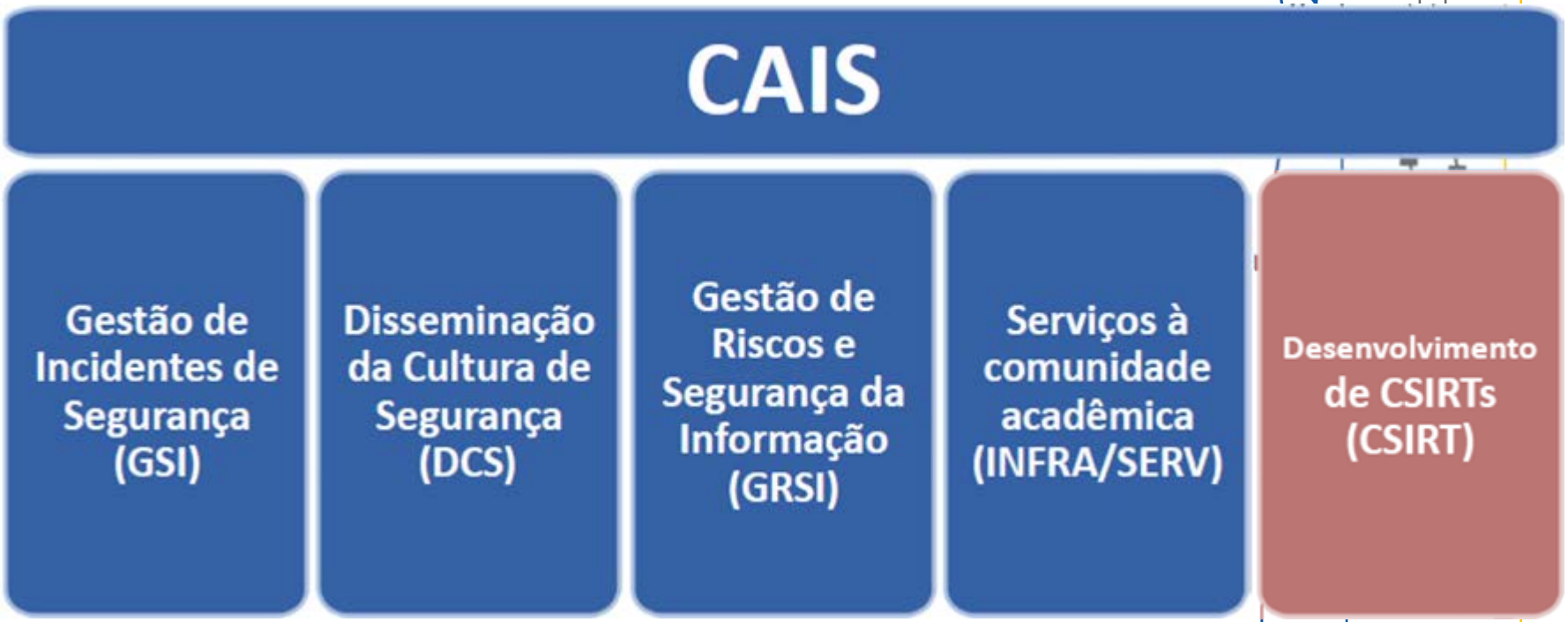
O CAIS

CAIS Centro de Atendimento a Incidentes de Segurança

19 anos de atuação na área de segurança da informação dentro da rede de ensino e pesquisa brasileira

O CAIS

Linhas de atuação



O PFSI

Programa de Fortalecimento em Segurança da Informação nas OUs

O PFSI

Programa de Fortalecimento em Segurança da Informação nas OUs

- Sistema de Gestão de Incidentes de Segurança (SGIS)
- Combate a Atividade Maliciosa
- Ações em Conscientização em Segurança
- Apoio na Elaboração de Políticas de Segurança
- **Apoio na criação de CSIRTs**

CSIRTs

Um *Computer Security Incident Response Team* (CSIRT) ou um Equipe de Tratamento de Incidentes de Rede (ETIR),

é uma equipe que responde a incidentes de segurança provendo suporte necessário para resolvê-los ou auxiliar na resolução.

CSIRTs

Demandas principais:

Criar um único ponto de contato na rede para comunicar incidentes de segurança.

Atuar de forma confiável no tratamento, resolução e resposta dos incidentes de segurança.

Motivação

Cenário desfavorável	Maré crescente de incidentes e vulnerabilidades críticas nos últimos anos.
Fortalecimento da segurança	Necessidade de aumentar a capacidade de segurança da informação na rede acadêmica.
Rede acadêmica	Atendimento a normas e disposições legais brasileiras, sobretudo para as organizações que fazem parte da APF.
Foco no tratamento dos incidentes	Equipe de segurança corporativa ≠ CSIRT

Motivação

PROJETO CSIRTs nos clientes da RNP

Objetivos

Projeto CSIRTs nos clientes da RNP

Criação de modelo	Criar um modelo padrão e genérico de estabelecimento de um novo CSIRT aplicável às realidades da rede de ensino e pesquisa.
Gestão de incidentes	Definir um modelo de gestão de incidentes de segurança, com processos e procedimentos para as fases do ciclo de tratamento de incidentes.
Guia	Disponibilizar um guia e um checklist para apoio no estabelecimento de um novo CSIRT.
Interação	Promover a interação entre as novas equipes de resposta a incidentes com as equipes já existentes.

Embasamento

Normas

ABNT ISO/IEC 27002:2013

Diretrizes para Gestão de incidentes de segurança.

- **Responsabilidades e procedimentos;**
- **Avaliação dos eventos de segurança da informação;**
- **Resposta aos incidentes de segurança da informação;**
- **Coleta de evidências.**

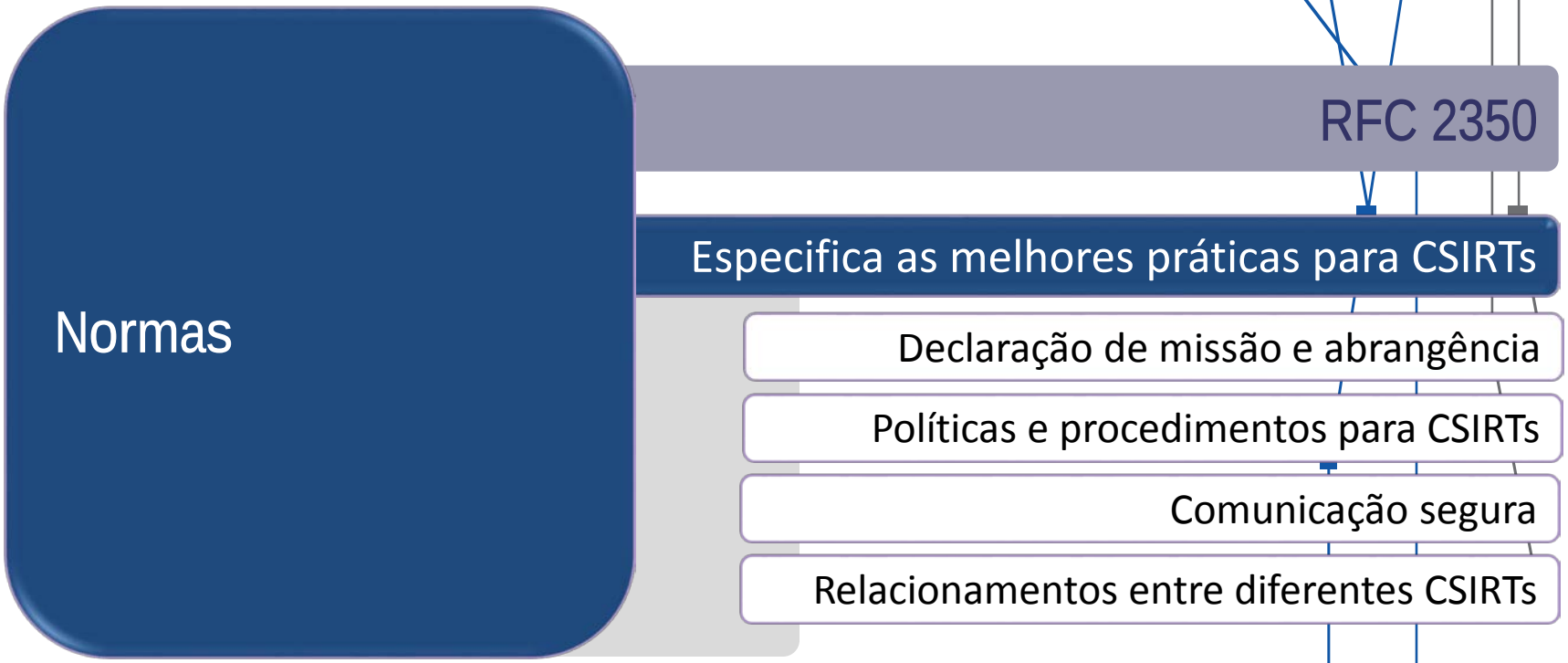
Embasamento

Normas

Instrução Normativa GSI/PR Nº 1:2008.

Norma Complementar nº 05/IN01/DSIC/GSIPR	Disciplina a criação da Equipe de tratamento e Respostas a Incidentes e Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal.
Norma Complementar nº 08/IN01/DSIC/GSIPR	Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes computacionais nos órgãos e entidades da Administração Pública Federal.

Embasamento



Embasamento

Normas

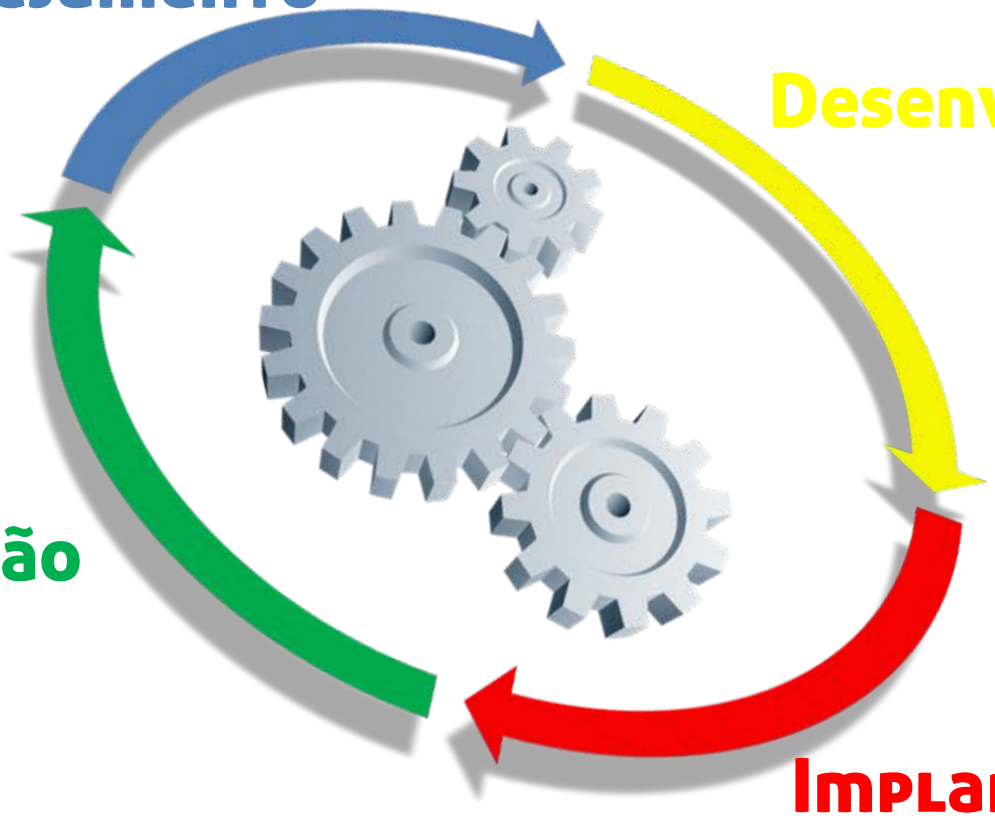
ABNT ISO/IEC 27035:2016

Diretrizes sobre gerenciamento de incidentes de segurança de informações e orientação para organizações externas que fornecem serviços de gerenciamento de incidentes de segurança de informações.

Por onde começar a montar Seu Hackbusters?

Metodologia

Planejamento



Desenvolvimento

Operação

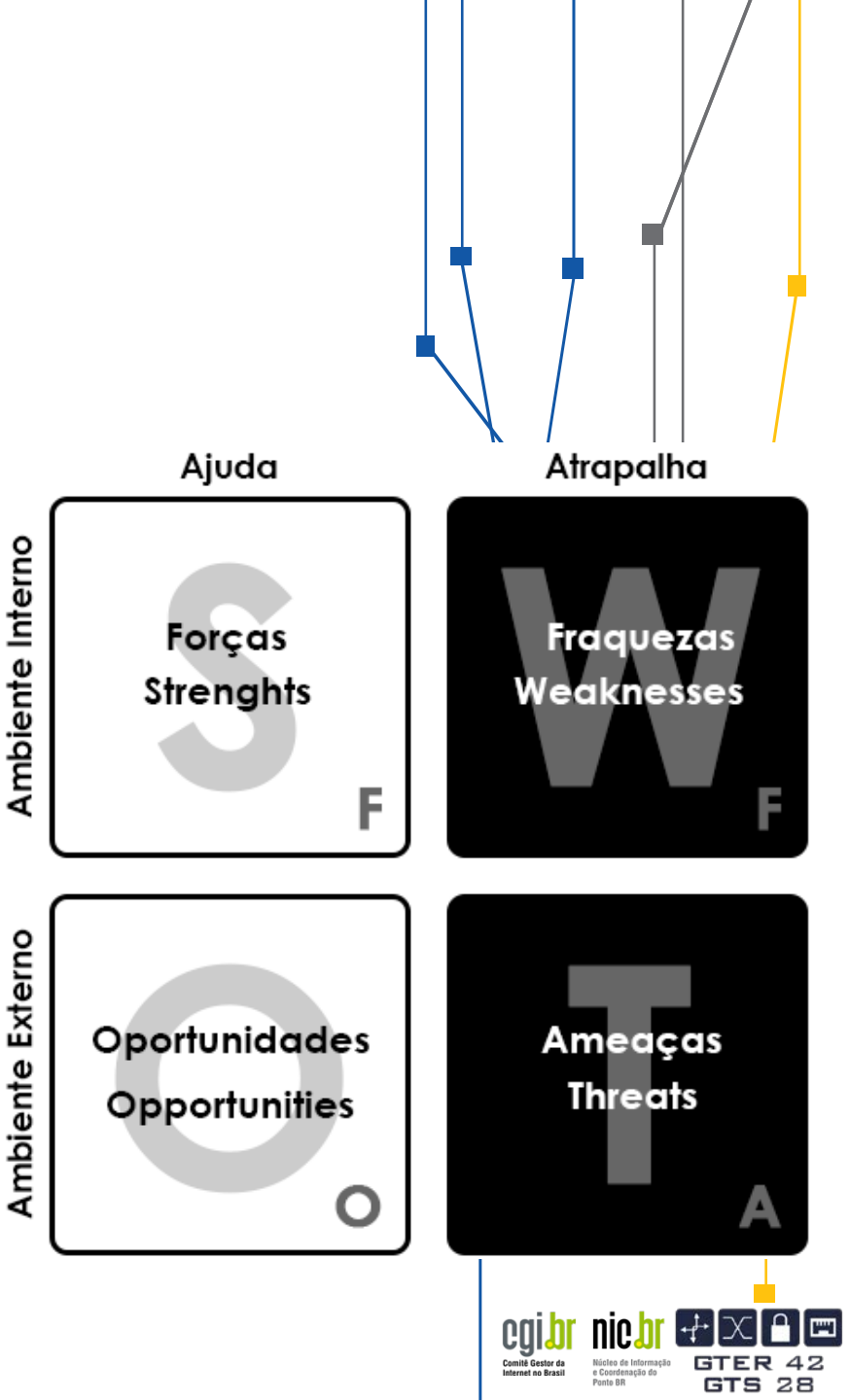
Implantação

Step 1: Planejamento

Matriz SWOT / FOFA

É uma metodologia utilizada para fazer análise de cenário de ambientes internos e externos em uma organização.

Análise de dados com o objetivo de posicionar estrategicamente uma organização em uma determinada questão.



Passo 1: Planejamento

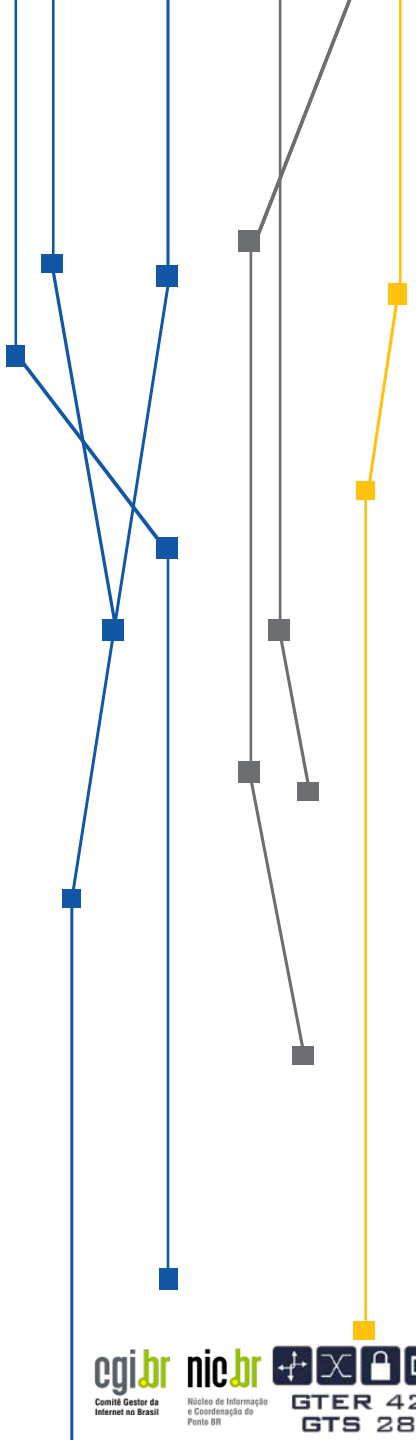
Stakeholders

- Equipe de projeto
- Alta administração
- Diretoria de TIC
- Comitê Gestor de TIC
- Setor Jurídico
- Setor de compras
- Equipe de TIC
- Servidores/funcionários
- Corpo discente

Passo 2: Desenvolvimento

Nome e sigla

O nome e a sigla permitem ao seu CSIRT criar uma identidade própria, que deve estar alinhada com a de sua instituição e, se possível, refletir o setor que representa (banco, indústria, governo etc.).



Passo 2: Desenvolvimento

Missão

- O que é
- Como fazer

6. DEFINIÇÃO DA MISSÃO

6.1 A missão deve fornecer uma breve e inequívoca descrição dos objetivos básicos e a função da Equipe de Tratamento e Resposta a Incidentes em Redes de Computadores. A definição da missão fornecerá a linha base para as atividades a serem desenvolvidas pela equipe.

Passo 2: Desenvolvimento

Missão

Use verbos no infinitivo / Use palavras-chave

- O que é
- Como fazer

coordenar

proteger

prevenir

garantir

promover

tratar

responder

incidentes de segurança

disseminação da cultura

segurança da informação

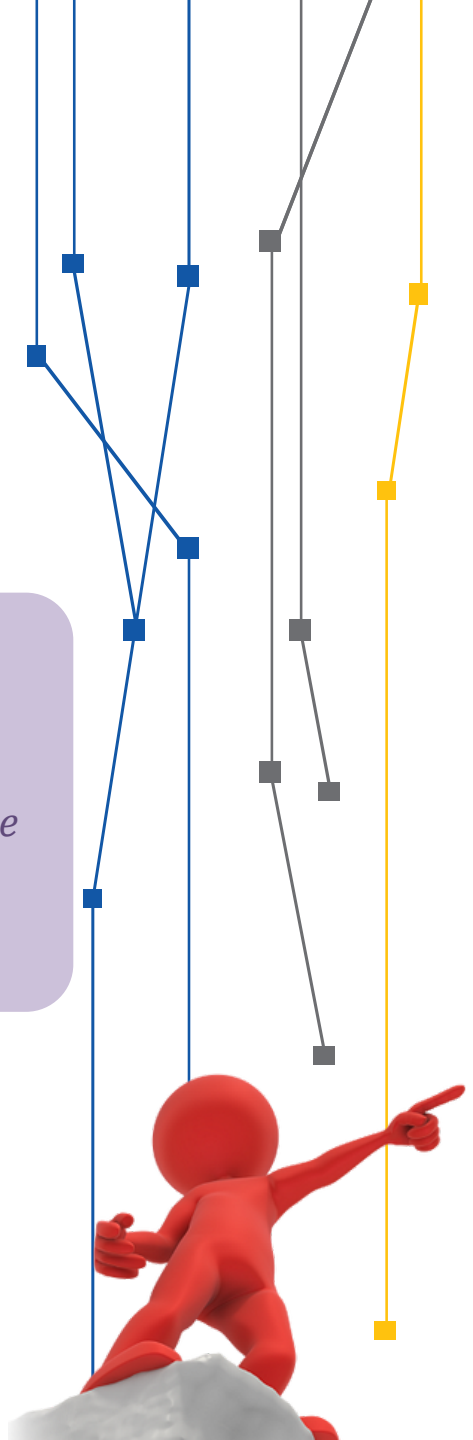
Passo 2: Desenvolvimento

Visão

- O que é

DEFINIÇÃO DA VISÃO

Definir os objetivos futuros, a orientação a longo prazo de onde se deseja chegar, como o CSIRT espera ser reconhecido pela organização.

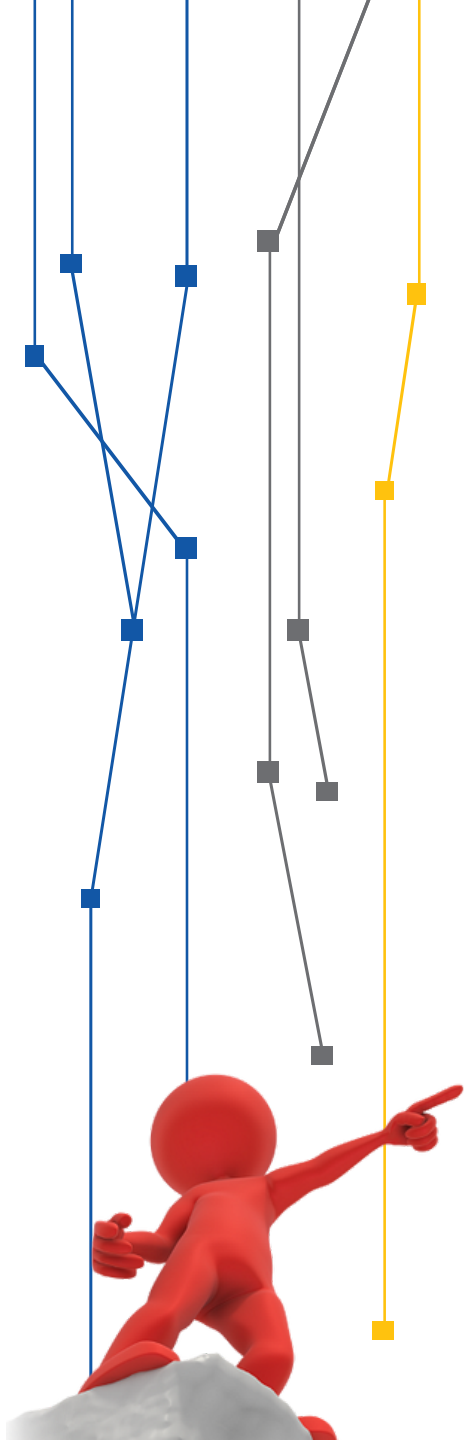


Passo 2: Desenvolvimento

Visão

- O que é
- Como fazer

Leve em consideração a cultura e a expectativa organizacional



Passo 2: Desenvolvimento

Constituency

- O que é

DEFINIÇÃO DO PÚBLICO ALVO

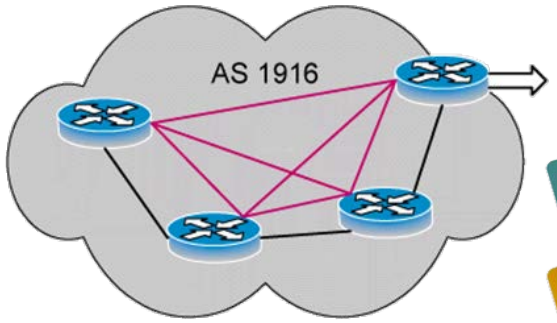
Quem são os clientes do CSIRT: quem a equipe vai atender, os diferentes tipos de usuários e/ou diferentes tipos de serviços.

Passo 2: Desenvolvimento

Constituency

Especifique de forma clara os diferentes tipos de usuários e/ou serviços

- Como fazer



Passo 2: Desenvolvimento

Serviços

- O que é

DEFINIÇÃO DE SERVIÇOS

Definir um conjunto de atividades que serão providos para os clientes: Como o CSIRT vai atender a organização?

Passo 2: Desenvolvimento

Serviços

- Como fazer

REATIVOS:

- ❑ *Gerenciamento de incidentes de segurança*
  - *Inclui "Tratamento de Incidentes de segurança"*
- ❑ *Análise forense de ambientes comprometidos*
- ❑ *Análise de artefatos*

Passo 2: Desenvolvimento

Serviços

- Como fazer

PROATIVOS:

- ❑ *Gerenciamento de vulnerabilidades*
  - *OpenVAS, Nmap, Lynis, MBSA, w3af.*
- ❑ *Monitoramento da rede*
  - *IDS: Snort, Suricata, OSSEC;*
  - *Honeypot: Honeyd, Nephentes;*
  - *Flows: NTOP, Wireshark;*
  - *SIEM: Splunk, OSSIM;*

Passo 2: Desenvolvimento

Serviços

- Como fazer

QUALIDADE:

- ***Gestão de riscos de segurança da informação***
- ***Gestão de conformidade (compliance)***
  - ***MSCM (Microsoft Security Compliance Manager);***
  - ***OpenSCAP (sistemas Linux);***
- ***Disseminação da cultura em segurança da informação;***

Passo 2: Desenvolvimento

Serviços

- Como fazer

Indicação de serviços iniciais:

- *Gerenciamento de Incidentes de segurança da informação*
- *Disseminação da cultura em segurança da informação*

Palavra-chave:
EVOLUÇÃO

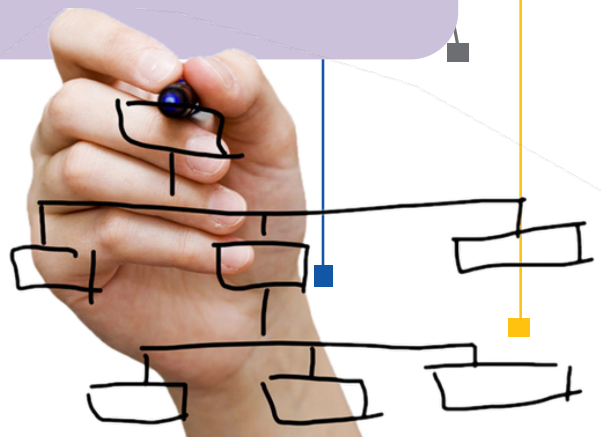
Passo 2: Desenvolvimento

Estrutura Organizacional

- O que é

DEFINIÇÃO DE ESTRUTURA ORGANIZACIONAL

Forma pela qual as atividades desenvolvidas pela equipe são divididas, organizadas e coordenadas.

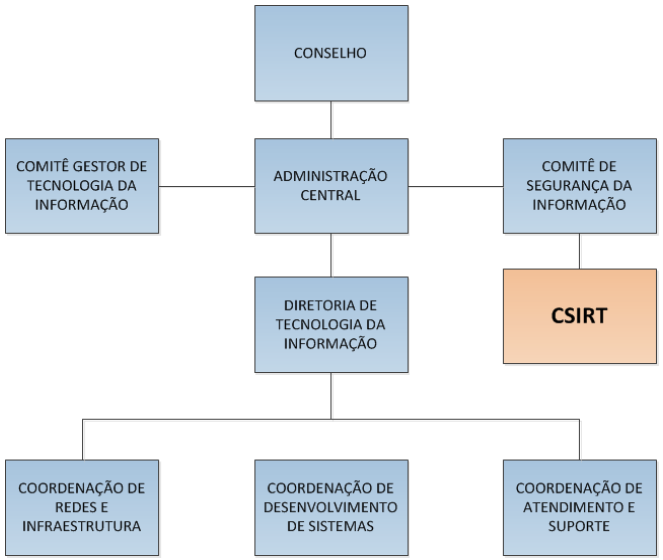


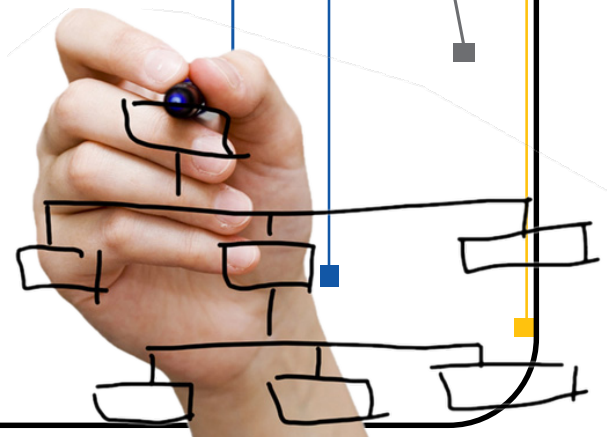
Passo 2: Desenvolvimento

Estrutura Organizacional

- Posição na organização

Exemplos: vinculado ao Comitê de Segurança da Informação



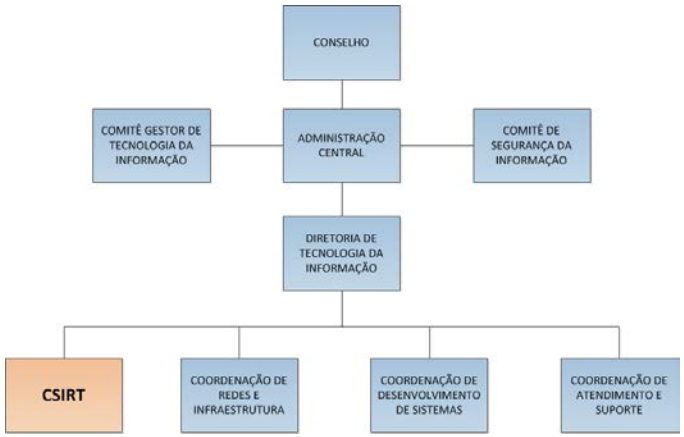


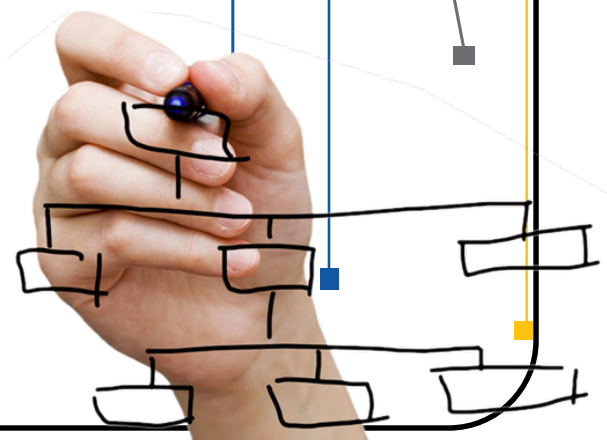
Passo 2: Desenvolvimento

Estrutura Organizacional

- Posição na organização

Exemplos: vinculado à Diretoria de TIC



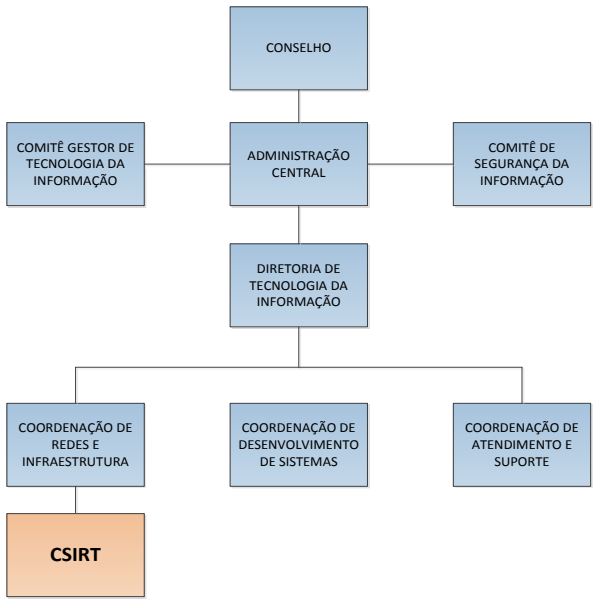


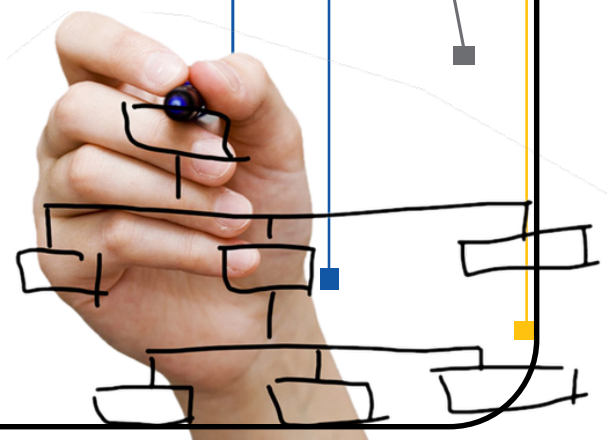
Passo 2: Desenvolvimento

Estrutura Organizacional

- Posição na organização

Exemplos: vinculado a uma Coordenação





Passo 2: Desenvolvimento

Estrutura Organizacional

- Organograma interno

Modelo básico de estrutura organizacional interna sugerido

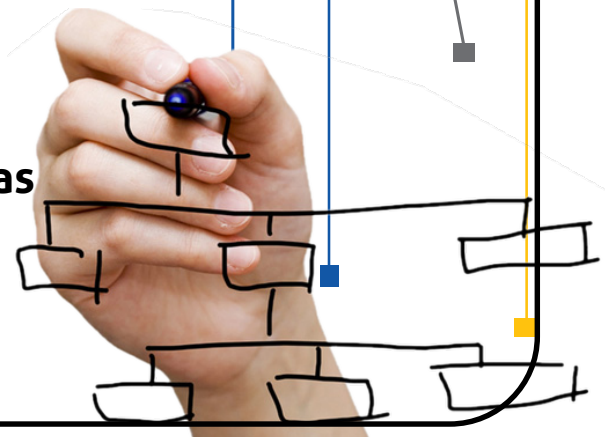
Passo 2: Desenvolvimento

Estrutura Organizacional

- Formação da equipe

Papéis e responsabilidades:

- Coordenação/Gestão
- Primeiro atendimento
- Triagem
- Análise e pesquisa
- Resposta a incidentes
- Comunicação
- Administração de redes e sistemas
- Equipe Jurídica
- Recursos Humanos
- Controle de qualidade



Passo 2: Desenvolvimento

Estrutura Organizacional

- Formação da equipe

Conhecimentos e responsabilidades:

Membros do CSIRT	
Conhecimentos	**Responsabilidades**
Princípios básicos de gestão de segurança da informação	Responder às notificações de incidentes de segurança encaminhadas ao CSIRT
Ameaças à segurança (*malwares*, DDoS, *phishing*, *sniffing*, etc.)	Notificar outras equipes quando identificado um ataque direcionado
Aplicações de rede e Internet	Analisar a causa raiz dos incidentes e realizar ações de correção para evitar a reincidência
Família de protocolos TCP e UDP	Manter a base de dados de informações consistente e atualizada
Sistemas operacionais	Preservar evidências ou artefatos maliciosos
Infraestrutura de rede e roteamento	Auxiliar o coordenador do CSIRT, quando requisitado ou necessário, em tomadas de decisão
Ferramentas de segurança (IDS, Firewall, etc.)	

Passo 2: Desenvolvimento

Estrutura Organizacional

- Formação da equipe

Conhecimentos e responsabilidades:

Coordenador do CSIRT	
Conhecimentos	**Responsabilidades**
Gestão de pessoas Gestão de processos, incluindo melhoria contínua Gerenciamento de incidentes de segurança da informação Governança de TIC Normas de segurança da informação, Instruções Normativas do Governo, legislação, família ABNT ISO/IEC 27000.	Ser o ponto de contato com os CSIRTs de coordenação Gerenciar as atividades, coordenar metodologias e procedimentos internos; Garantir a operação das atividades no que se refere a recursos e infraestrutura; Representar o CSIRT em reuniões e foros internos; Ser o responsável junto às autoridades sobre incidentes que se tipifiquem crime; Responder por todas as decisões, ações técnicas e administrativas;

Passo 2: Desenvolvimento

Autonomia

- O que é

DEFINIÇÃO DA AUTONOMIA

Define o nível de competências e obrigações do CSIRT em processos de decisão sobre ações de tratamento e recuperação de incidentes.

Passo 2: Desenvolvimento

Autonomia

- Tipos

COMPLETA:

- *Não necessita de aprovação de níveis superiores; a equipe tem autoridade para tomar as medidas necessárias.*

COMPARTILHADA:

- *CSIRT faz parte de um colegiado responsável por tomar decisões.*

SEM AUTONOMIA:

- *CSIRT não tem autoridade, somente notifica, fornece orientações e informações.*

Passo 3: Implantação

1) Infraestrutura

2) Gestão de pessoas

3) Financiamento

4) Políticas, normas e procedimentos

Passo 3: Implantação

Infraestrutura

- Infraestrutura física

Passo 3: Implantação

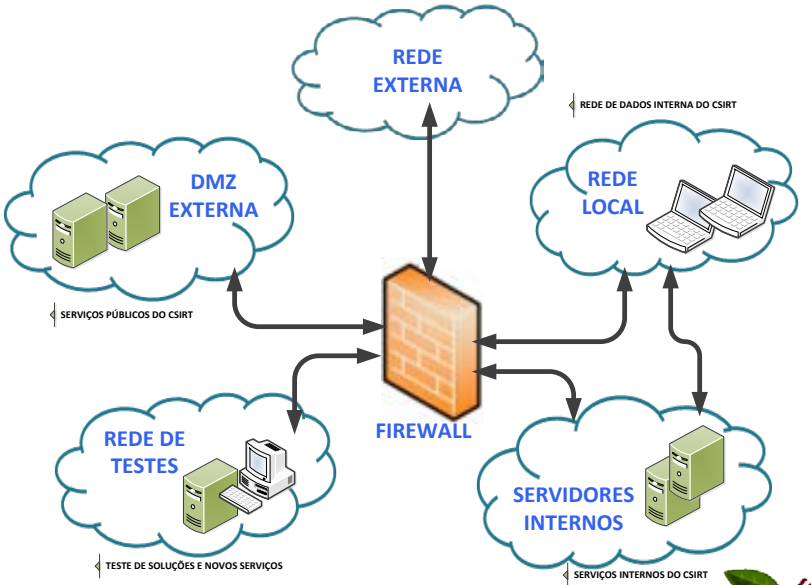
Infraestrutura

- Software e sistemas

Passo 3: Implantação

Infraestrutura

- Rede de dados



- Rede externa
- DMZ
- Servidores internos
- Rede de testes
- LAN

Passo 3: Implantação

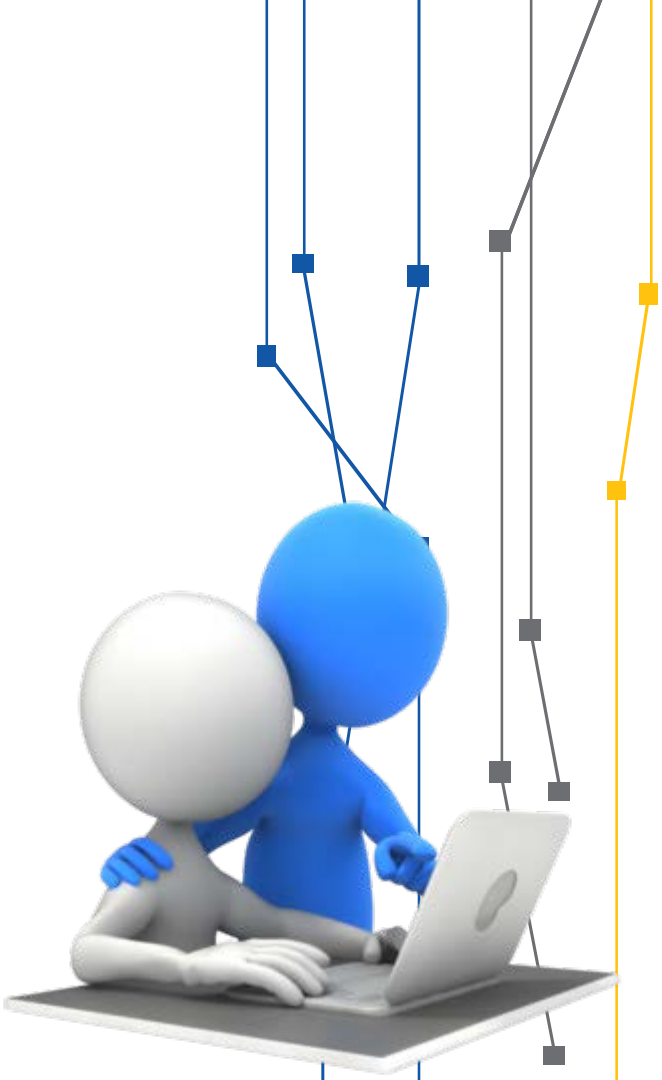
Gestão de Pessoas

Contratação

- Análise curricular
- Entrevista
- Definições contratuais
  * Plano de carreira
  * Carga horária (8x5? 24x7? Fins de semana?)
  * Disponibilidade para viagens
- Ética no trabalho

Passo 3: Implantação

Gestão de Pessoas



Desenvolvimento

- Acompanhamento / coaching
- Participação em eventos
- Capacitação

Passo 3: Implantação

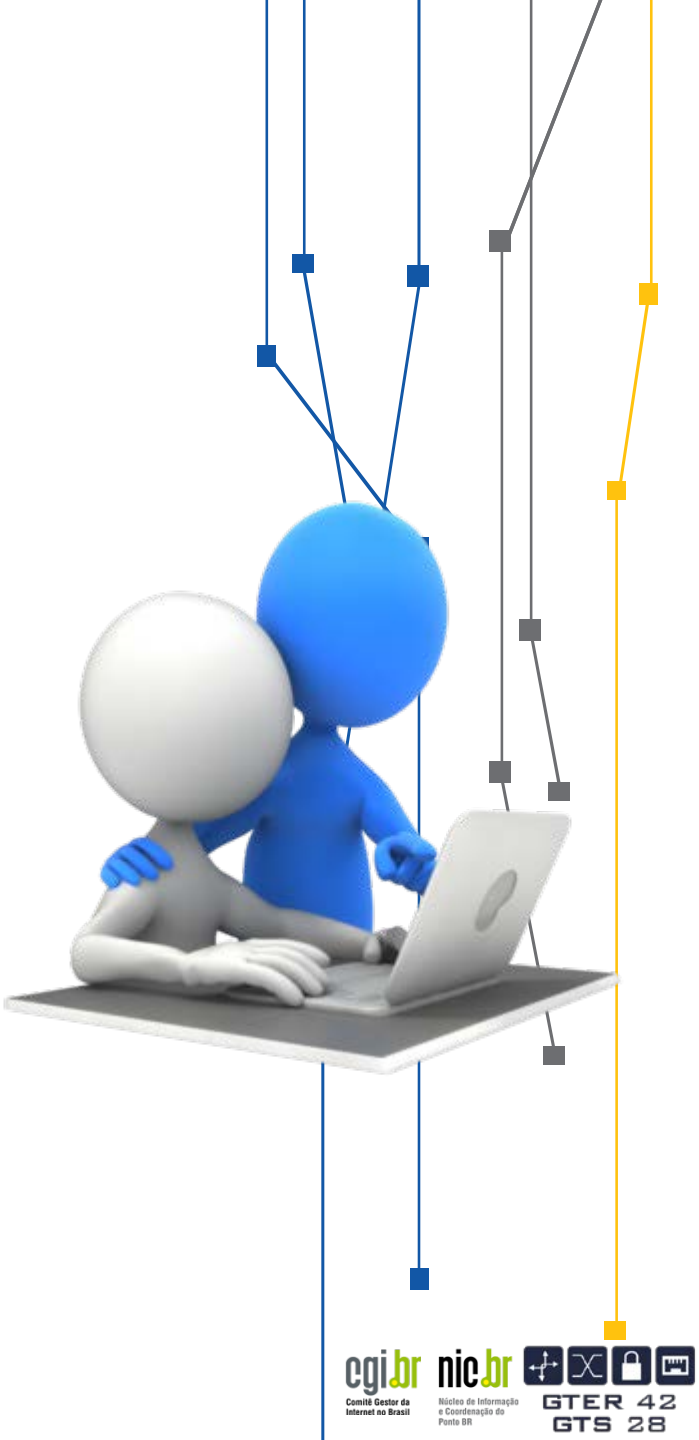
Gestão de Pessoas

Desenvolvimento

- Acompanhamento / coaching
- Participação em eventos
  * Fórum Brasileiro de CSIRTs
  * SBSeg
  * GTS NIC.br
  * Security Leaders
  * Roadsec
- Capacitação

Passo 3: Implantação

Gestão de Pessoas



Desenvolvimento

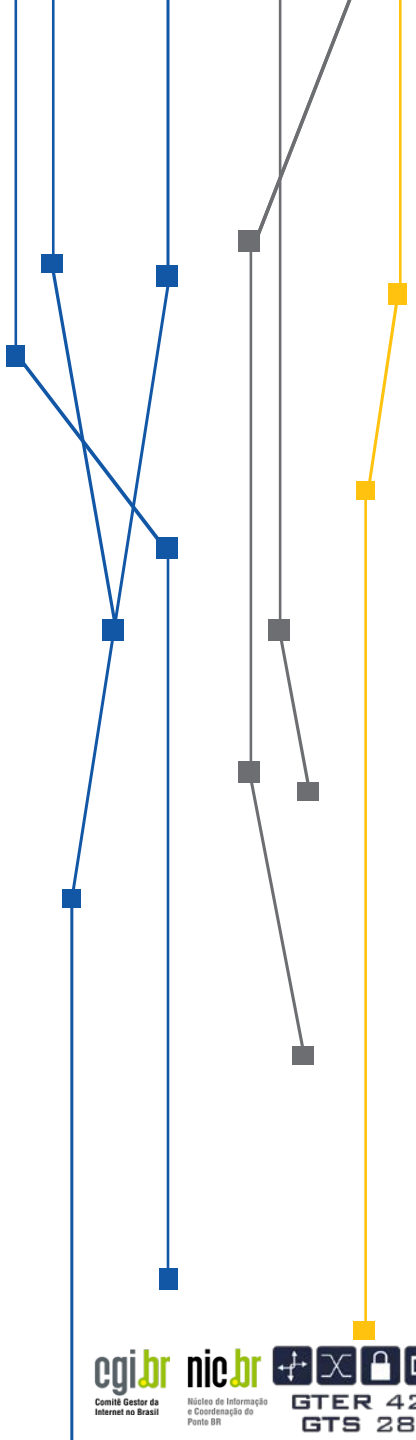
- Acompanhamento / coaching
- Participação em eventos
- Capacitação
  - * Escola Superior de Redes/RNP
  - * H2HC
  - * YSTS

Passo 3: Implantação

Gestão de Pessoas

Desligamento

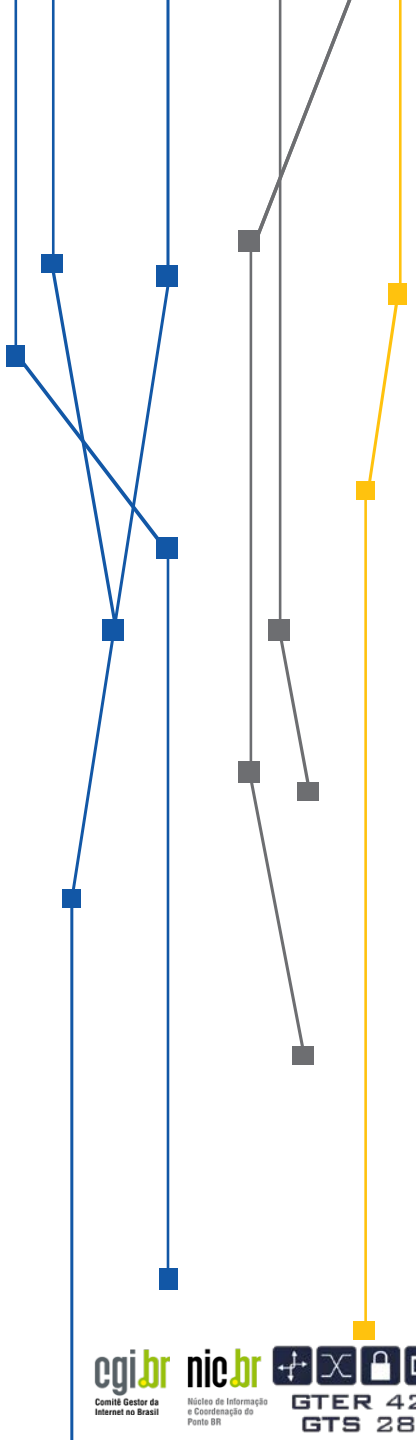
- Conta de usuário
- Credenciais de acesso
- Dados pessoais
- E-mail corporativo
  * Notificação à organização



Passo 3: Implantação

Financiamento

- Orçamento para CSIRT?
- Utilizar verba da SegTIC?
- Outras formas?
  * Parcerias com outras instituições
  * “Venda” de serviços à comunidade
  * Submissão de projetos para fundos de fomento à pesquisa



Passo 3: Implantação

Políticas/Normas/Procedimentos

Classificação da Informação

Passo 3: Implantação

Políticas/Normas/Procedimentos

Tratamento da Informação

Passo 3: Implantação

Políticas/Normas/Procedimentos

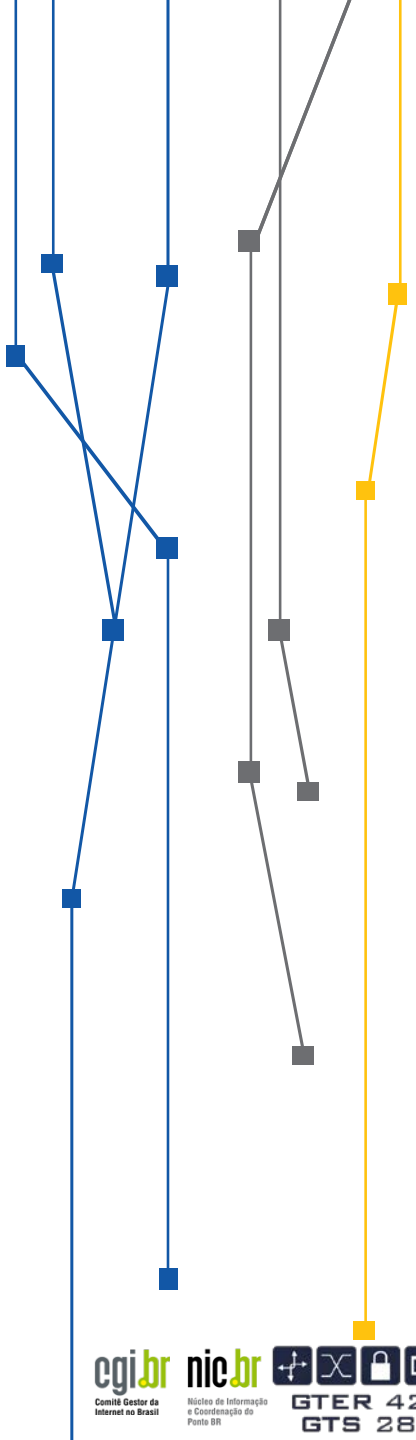
Normas de uso de recursos

Passo 3: Implantação

Políticas/Normas/Procedimentos

Política de senhas

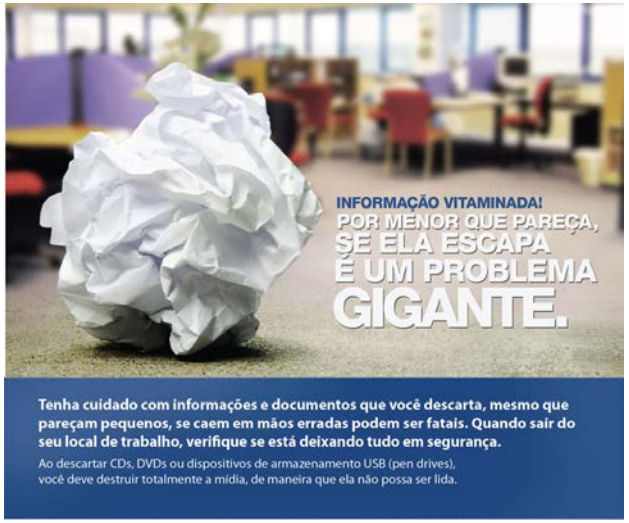
Plano de Comunicação



Passo 3: Implantação

Políticas/Normas/Procedimentos

Plano de Disseminação da Cultura em Segurança



Campanhas de conscientização

Passo 3: Implantação

Políticas/Normas/Procedimentos

Plano de Disseminação da Cultura em Segurança

Treinamentos técnicos

Passo 3: Implantação

Políticas/Normas/Procedimentos

Plano de Disseminação da Cultura em Segurança

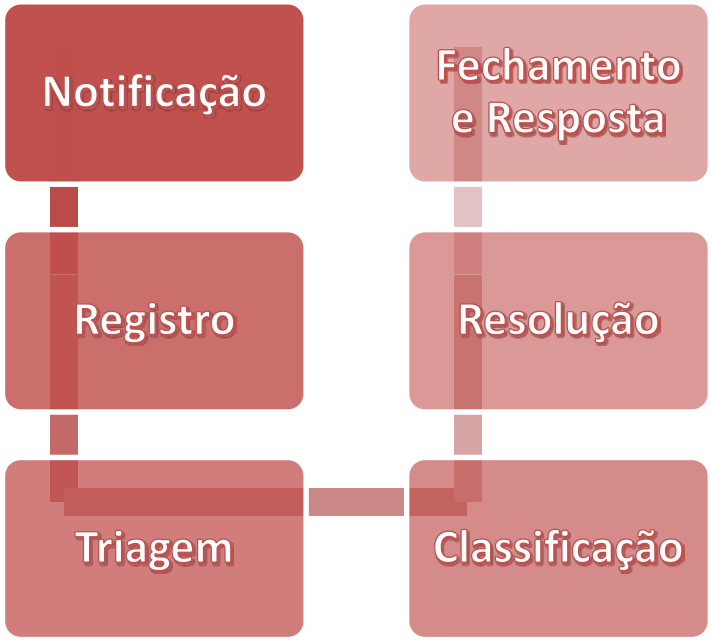
Boletins de notícias e dicas de segurança

Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:



Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:

Notificação

- Meios de notificação de incidente
  - Canais de comunicação;
  - Formas de detecção de atividades maliciosas;
- Elementos de uma notificação de incidente
  - Descrição do incidente
  - IP origem / destino
  - Portas / protocolos / serviços afetados
  - Horário (com GMT)

Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:

Registro

- Como os incidentes serão registrados;
  - Sistema de registro tickets
  - Outros;
- Identificador único;
- Confirmação de que a notificação foi recebida;
  - Informação de que o incidente foi encaminhado para tratamento

Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:

Triagem

- Se a notificação É um incidente de segurança
  - Validação do autor;
  - Validação da descrição do incidente;
  - Notificação com as informações necessárias;
- O que fazer com a notificação
  - Descartar notificação;
  - Reencaminhar a outra organização;
  - Seguir o fluxo de resolução;

Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:

Classificação

- Taxonomia
  - Tabela de tipos e subtipos de incidentes;
- Criticidade
  - A nível técnico e a nível de negócios;
- Status
  - Aberto / Fechado / Status intermediários;

Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:

Resolução

- Escalar responsável pelo tratamento;
- Ciclo básico de resolução do incidente:

Passo 3: Implantação

Gestão de incidentes

Plano de Gestão de Incidentes

Seis etapas principais:

Fechamento e Resposta

- Resposta ao incidente:
  - Informações necessárias ao responder um incidente de segurança;
  - A quem deve ser enviada a resposta ao encerrar o tratamento;

Passo 3: Implantação

Gestão de incidentes

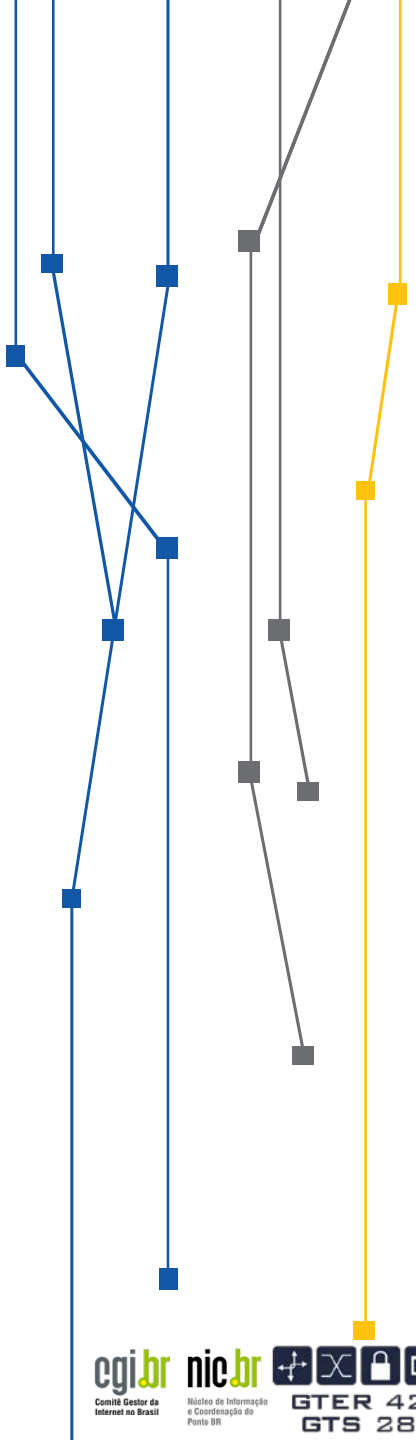
Plano de Gestão de Incidentes

Ações pós-incidente

Passo 3: Implantação

Gestão de incidentes

Procedimentos



Passo 4: Operação

1) Formalização

2) Divulgação

3) Análise crítica

Passo 4: Operação

Formalização

[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 mento 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
.

Passo 4: Operação

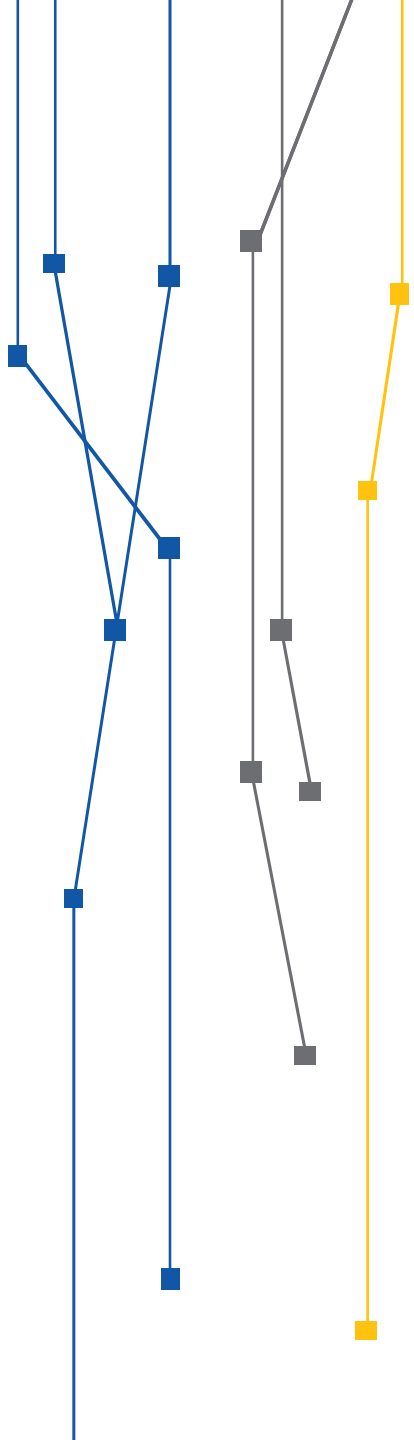
Divulgação

Passo 4: Operação

Análise crítica

Estatísticas

- Incidentes por período
- Incidentes por categoria
- Período de maior ocorrência de incidentes
- Protocolos mais usados
- Endereços IP’s envolvidos



Passo 4: Operação

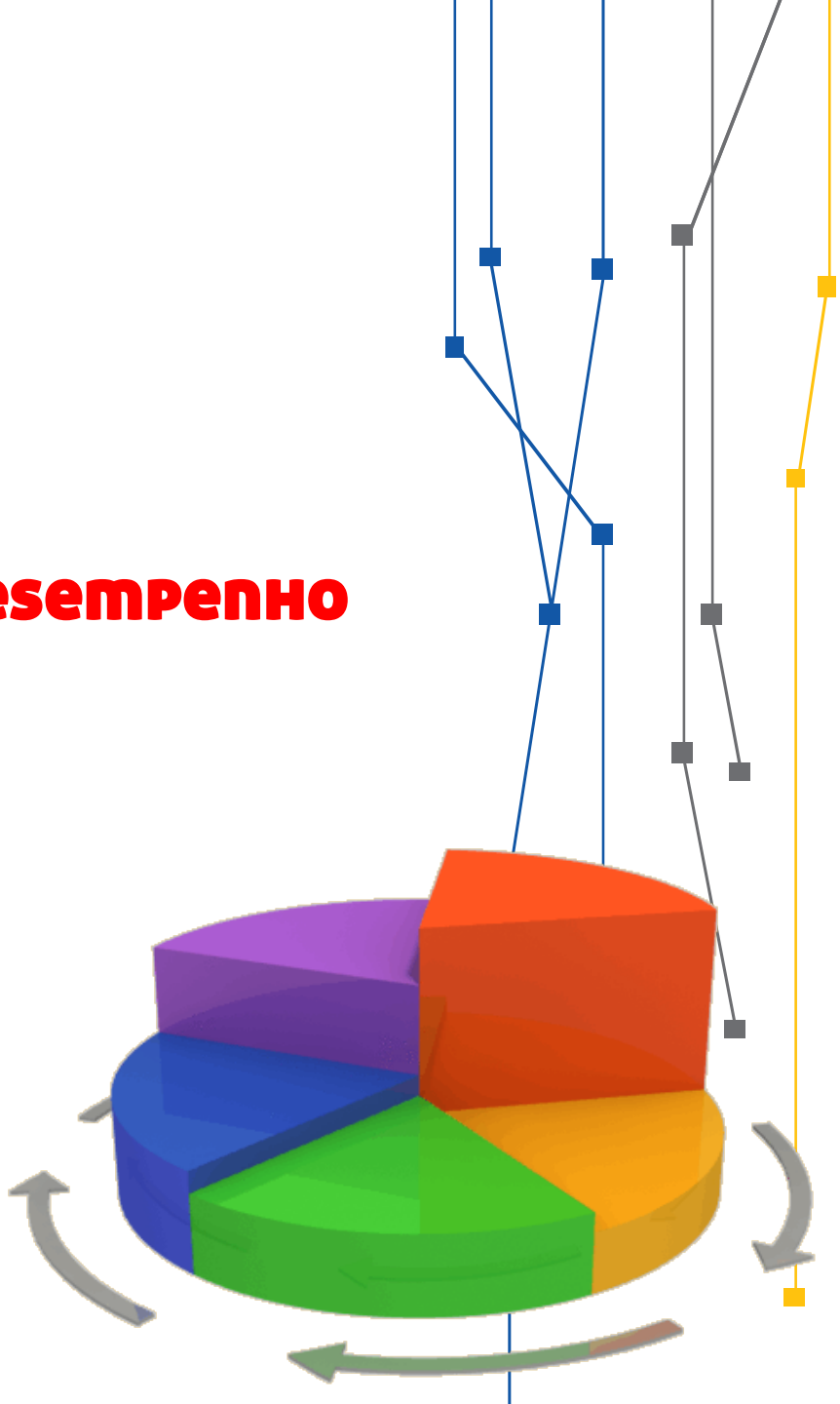
Análise crítica

Indicadores de desempenho

- Metas
  * Incidentes resolvidos dentro do SLA
  * Incidentes fechados durante período

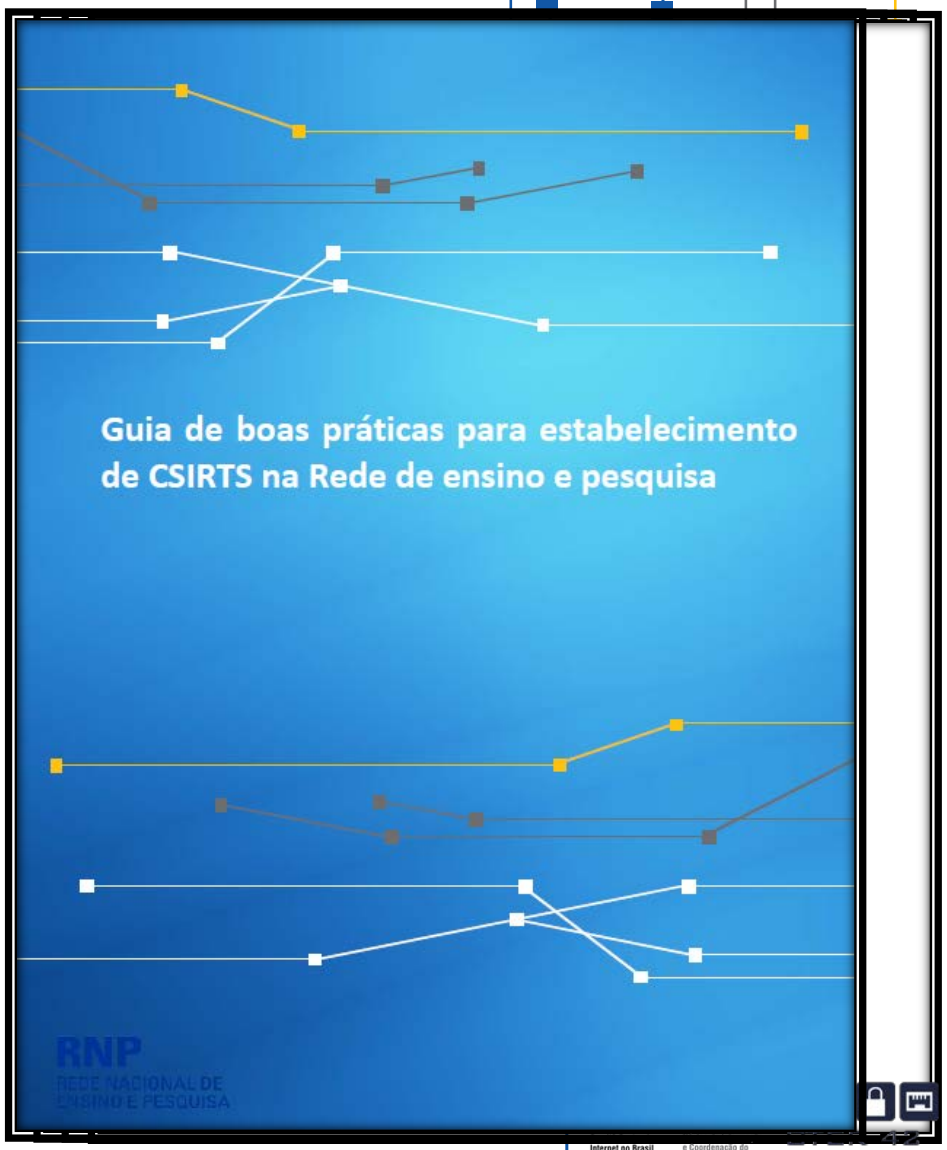
- Periodicidade
  Ex: diária, semanal, mensal, sob demanda

- Medição / Cálculo
  Ex: manual, sistema



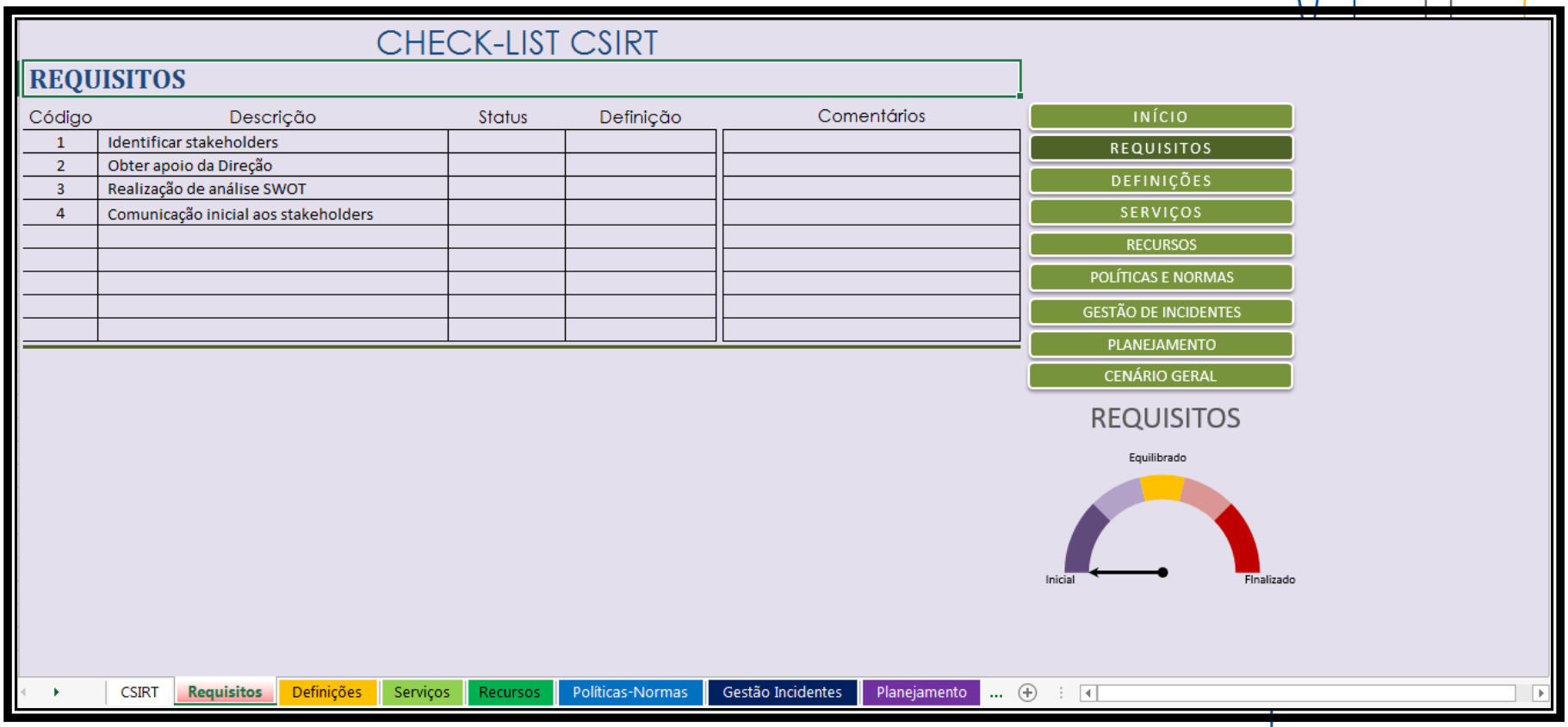
Resultados

– Guia de boas práticas para estabelecimento de CSIRTs na Rede de Ensino e Pesquisa



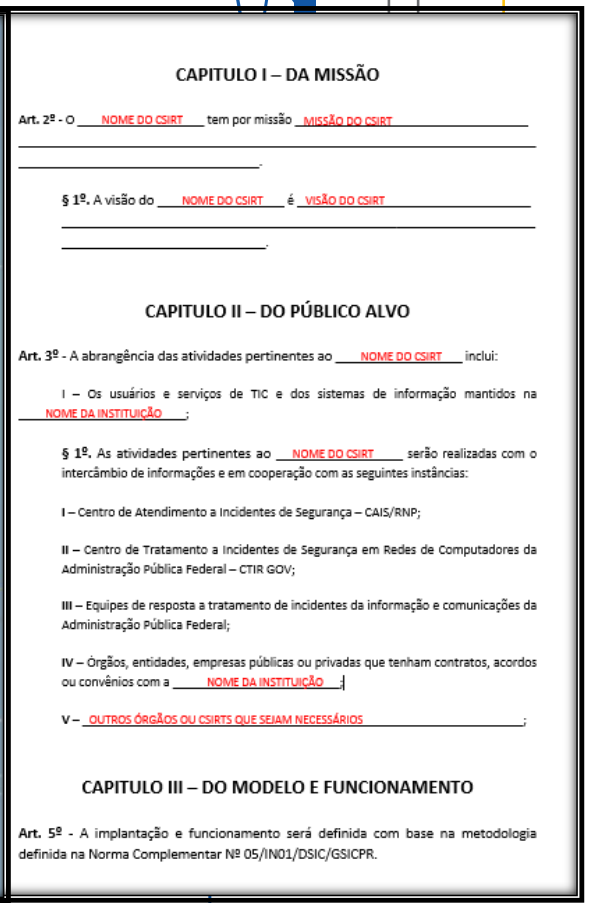
Resultados

– Checklist



Resultados

– Modelos



CAPITULO I – DA MISSÃO

Art. 2º - O NOME DO CSIRT tem por missão MISSÃO DO CSIRT.

§ 1º. A visão do NOME DO CSIRT é VISÃO DO CSIRT.

CAPITULO II – DO PÚBLICO ALVO

Art. 3º - A abrangência das atividades pertinentes ao NOME DO CSIRT inclui:

I – Os usuários e serviços de TIC e dos sistemas de informação mantidos na NOME DA INSTITUIÇÃO;

§ 1º. As atividades pertinentes ao NOME DO CSIRT serão realizadas com o intercâmbio de informações e em cooperação com as seguintes instâncias:

I – Centro de Atendimento a Incidentes de Segurança – CAIS/RNP;

II – Centro de Tratamento a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV;

III – Equipes de resposta a tratamento de incidentes da informação e comunicações da Administração Pública Federal;

IV – Órgãos, entidades, empresas públicas ou privadas que tenham contratos, acordos ou convênios com a NOME DA INSTITUIÇÃO;

V – OUTROS ÓRGÃOS OU CSIRTS QUE SEJAM NECESSÁRIOS;

CAPITULO III – DO MODELO E FUNCIONAMENTO

Art. 5º - A implantação e funcionamento será definida com base na metodologia definida na Norma Complementar Nº 05/IN01/DSIC/GSICPR.

Resultados

Novos CSIRTs:

Piloto realizado em 4 Organizações

Cases de sucesso:

UFBA

Salvador/BA

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FARROUPILHA

Santa Maria/RS

Resultados

TRIIF – Time de Resposta a Incidentes do Instituto Federal Farroupilha

Resultados

UFBA – Universidade Federal da Bahia

Superintendência de Tecnologia da Informação | **UFBA**

PLANO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

https://gsic.ufba.br

1 Objetivo

Este plano de gestão de incidentes de segurança da informação visa garantir o tratamento e resposta eficazes aos eventos de segurança da informação que afetam a disponibilidade, integridade, confidencialidade ou autenticidade associados aos ativos e sistemas de informação e comunicações da UFBA. Além disso, o plano tem por objetivo definir funções e responsabilidades, documentar as ações e medidas necessárias para o tratamento de incidentes de forma rápida e eficiente, limitando seu impacto, e, assim, protegendo os ativos e as informações.

2 Papéis e Responsabilidades

- **Gestor de Segurança da Informação e Comunicações da UFBA:** responsável pelas ações de segurança da informação e comunicações na organização.
- **Equipe de Tratamento de Incidentes de Redes (ETIR-UFBA)**: responsável por receber, analisar, tratar ou apoiar o tratamento e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores no ambiente da Universidade Federal da Bahia.
- **Coordenador da ETIR-UFBA:** responsável por gerenciar os membros e as atividades da equipe de resposta a incidentes.
- **Central de Serviços**: ponto de contato para recebimento de notificações de incidentes internos.
- **Administrador de rede ou de sistema**: responsável por investigar e tratar os incidentes de segurança, executando ações de análise e detecção do incidente, contenção, erradicação, recuperação e avaliação crítica, reportando-se à ETIR-UFBA sobre ações executadas e atualizando-a sobre mudanças nos contatos de redes ou sistemas.

3 Processo de Tratamento de Incidentes de Segurança da Informação

O processo de tratamento de incidentes de segurança da UFBA possui diversas fases e cada uma dessas fases possui um conjunto de entradas e saídas, ações e papéis, cuja execução ocorre sobre responsabilidade da Equipe de Tratamento de Incidentes de Redes da UFBA (ETIR-UFBA) com base no fluxo da Figura 1.

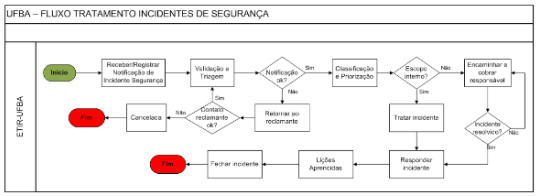


Fig. 1: Fluxo de Tratamento de Incidentes de Segurança da ETIR-UFBA

O fluxo de tratamento de incidentes de segurança apresentado acima será detalhado a seguir.

3.1 Notificação de Incidente de Segurança

3.1.1 Recebimento de Notificações

Serão considerados os seguintes meios para o recebimento de notificações de incidentes de segurança relacionados à UFBA:

- **Central de Serviços de TI da UFBA**, para incidentes de segurança reportados pelos usuários da comunidade UFBA, através dos seguintes contatos:
  - Telefone: (71) 3283-6100
  - E-mail: helpdesk@ufba.br
  - Web: https://webdesk.ufba.br
- **Contato do ETIR-UFBA**, para grupos de segurança ou reclamantes externos, através dos seguintes contatos:
  - Telefone: (71) 3283-6112
  - E-mail: security@ufba.br

As notificações devem conter evidências do incidente de segurança sendo reportado, bem como informações de contato do reclamante e dados adicionais que possibilitem melhor classificação e priorização do incidente.

3.1.2 Envio de Notificações

Os incidentes de segurança enviados pelo ETIR-UFBA para equipes ou órgãos internos ou externos devem conter um conjunto mínimo de informações que possibilite seu tratamento adequado pelo responsável. As notificações serão enviadas prioritariamente por e-mail, através da conta **etir@ufba.br**. Abaixo são relacionadas algumas informações que devem estar presentes:

- **Contato do ETIR**: as notificações devem conter informações de contato do ETIR-UFBA, a fim de facilitar a resposta ao incidente. Recomenda-se incluir as seguintes informações: telefone, e-mail, chave de criptografia, web site, sigla e nome do ETIR-UFBA;
- **Informações de origem do incidente**: endereço IP, URL do site ou recurso que originou o incidente; protocolos e portas utilizados pela origem do incidente; registro do tempo da ocorrência do incidente (data, horário e *time zone*);
- **Informações do alvo do incidente**: endereço IP, URL do site ou recurso que foi alvo do incidente; protocolos e portas utilizados no destino do incidente; registro do tempo da ocorrência do incidente (data, horário e *time zone*);
- **Descrição do incidente**: breve descrição do incidente, tais como tipo do ataque, motivação aparente, ou outras características relevantes;
- **Logs ou evidências**: deve-se incluir anexos com trechos de registros de eventos (*logs*), capturas de telas, códigos de erro ou outros registros que evidenciem a ocorrência do incidente.

As notificações de incidente de segurança da informação enviadas pelo ETIR-UFBA que estejam relacionadas à ativos externos (e.g. host de outras instituições, incidente envolvendo terceiros etc) devem acrescentar algumas entidades ou grupos de segurança que possuem relação com a instituição em diferentes contextos:

- CAIS/RNP <cais@cais.rnp.br>: O CAIS é o Centro de Atendimento a Incidentes de

Obrigado!

RNP

Ministério da
Cultura

Ministério da
Saúde

Ministério da
Educação

Ministério da
Ciência, Tecnologia e Inovação