Developing CSIRTs in Brazilian NREN

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**

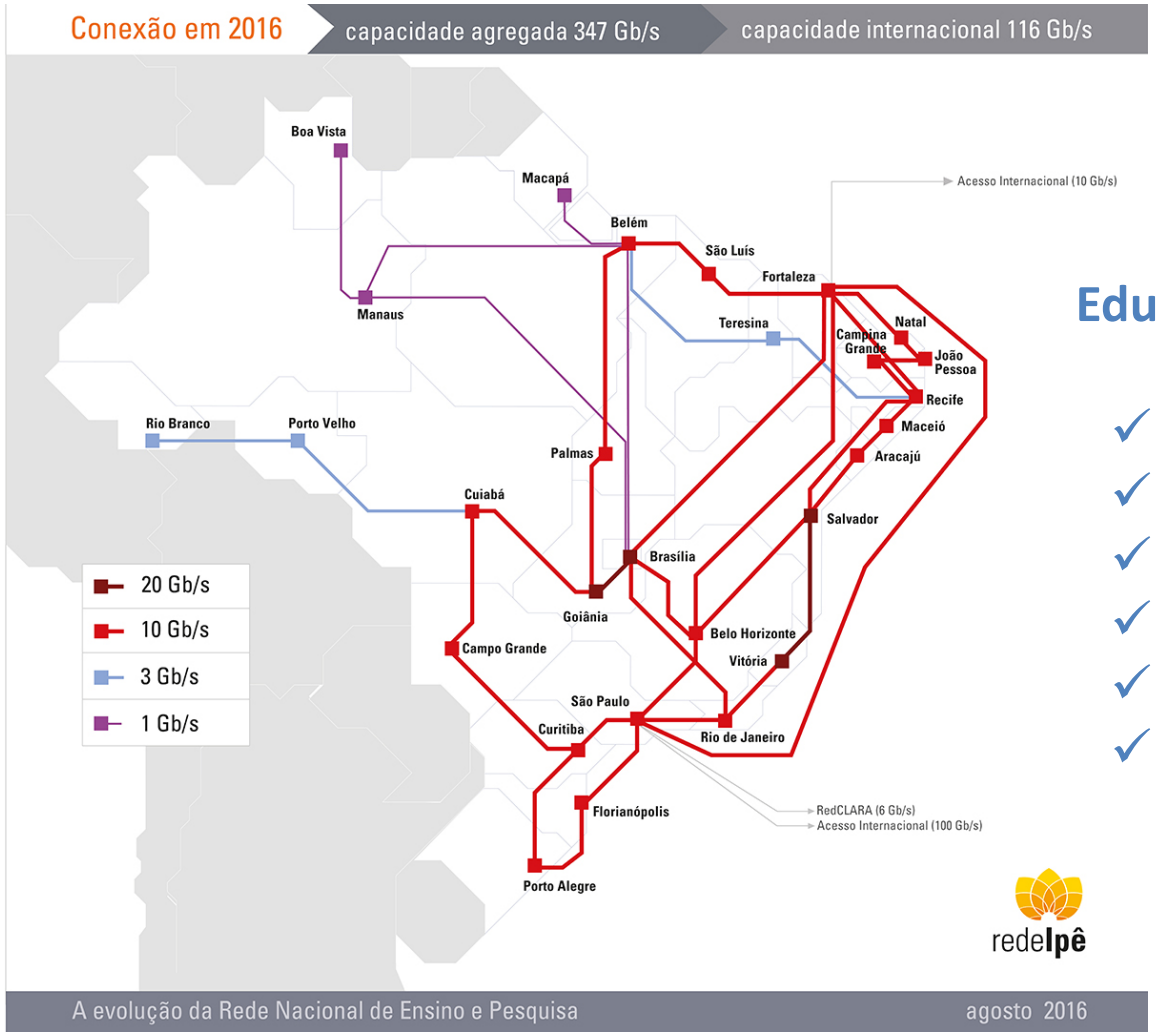
lacnic 27

22/26 mayo 2017 - foz do iguaçu, brasil

lacnic Seguridad en Redes

RNP

Mission: To promote the innovative use of advanced networks.

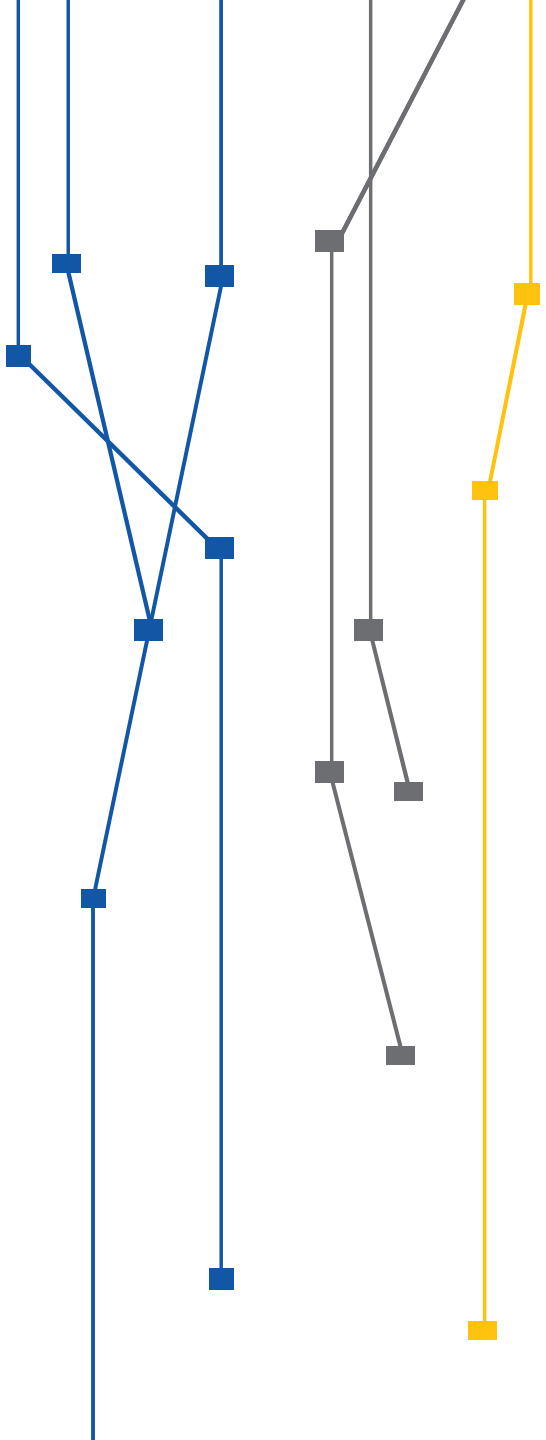


Education and research community:

- ✓ Universities;
- ✓ National Libraries;
- ✓ Research Institutes;
- ✓ Museums;
- ✓ Teaching hospitals;
- ✓ Others;

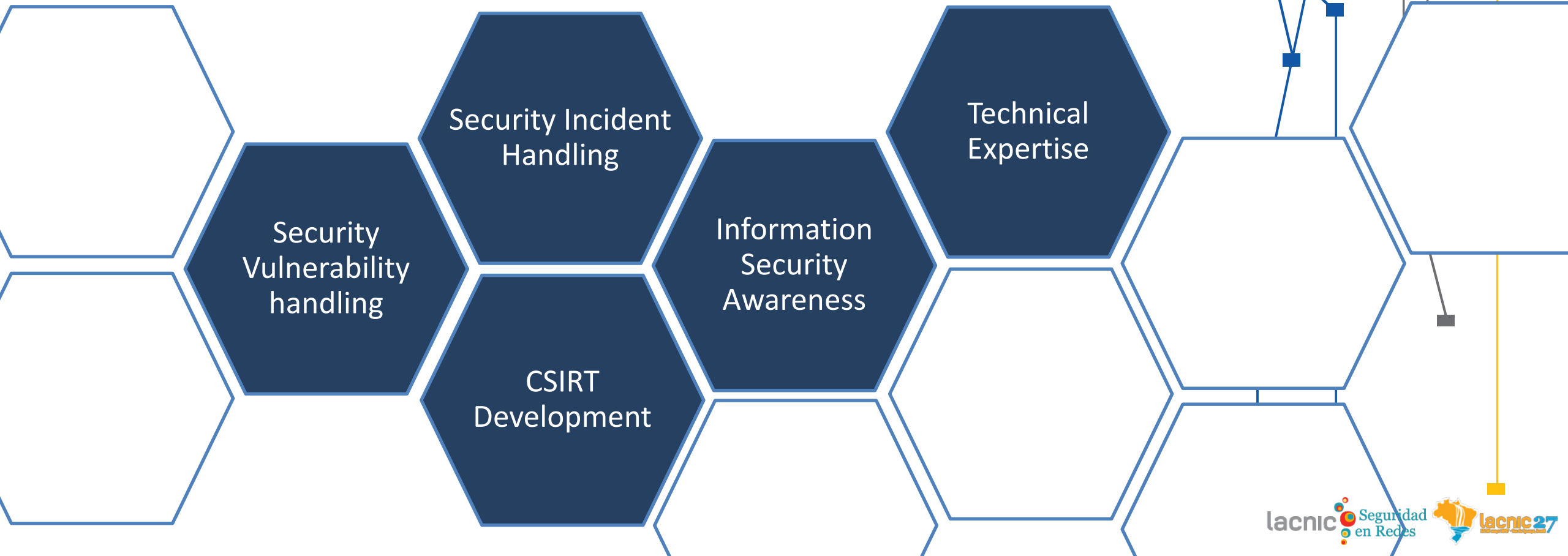
lacnic Seguridad en Redes lacnic27

CAIS



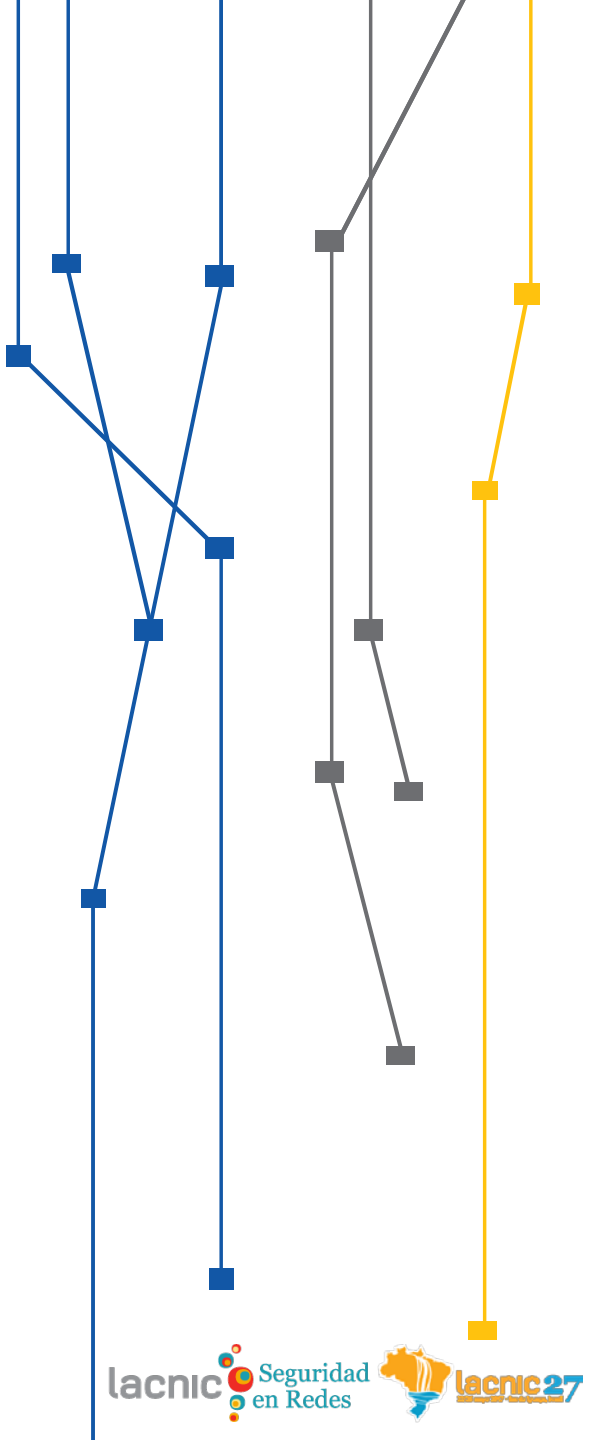
CAIS

Lines of action



PFSI

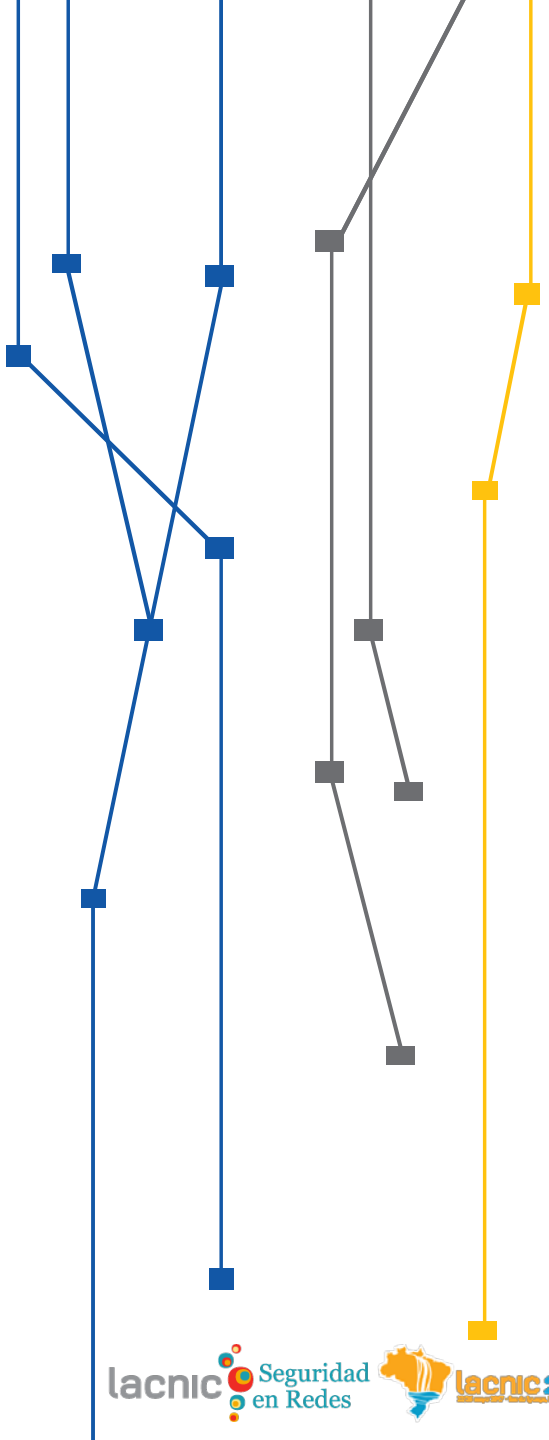
Information Security Strengthening Program in RNP Customers



PFSI

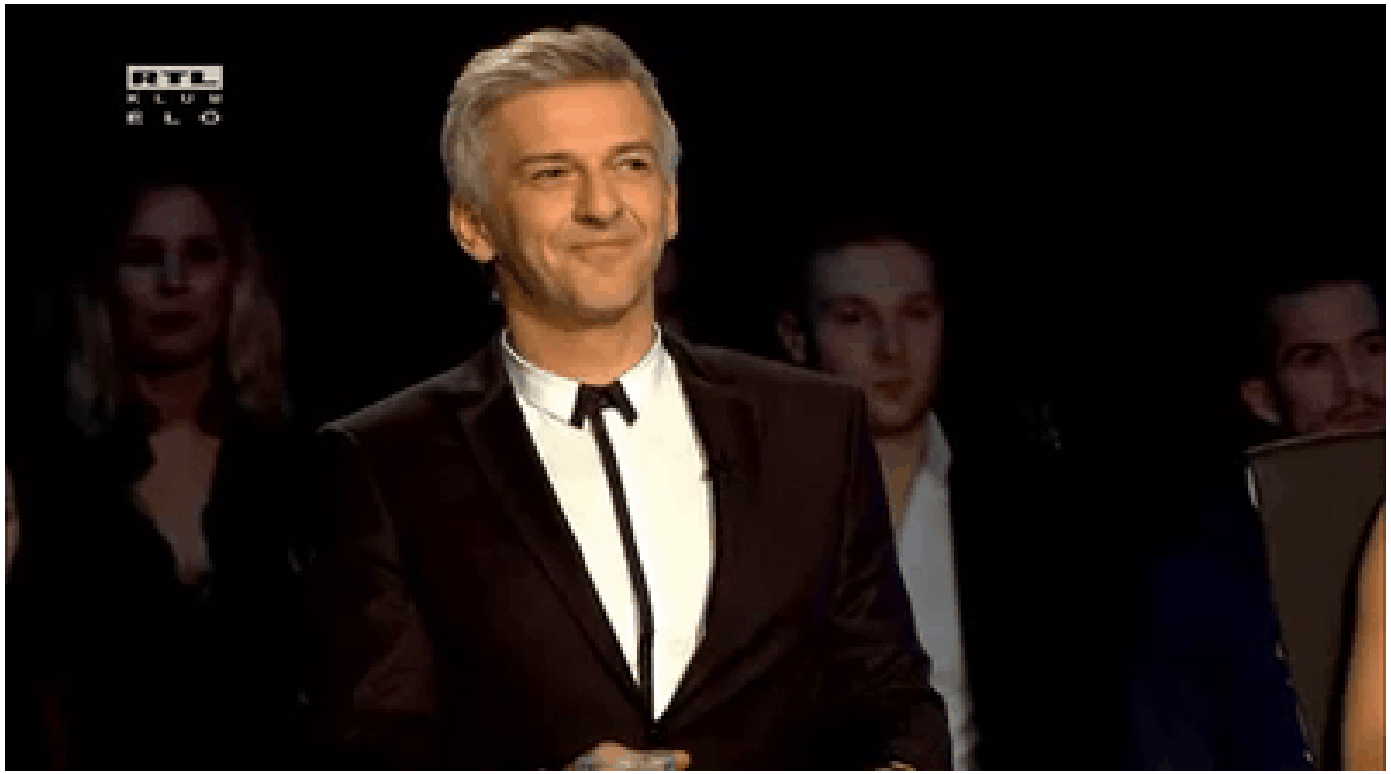
Information Security Strengthening Program in RNP Customers

- Incident Security Management System (SGIS)
- Malicious Activity Combat
- Security Awareness Actions
- Support to Develop Security Policy Documents
- **Support to Create and Develop CSIRTs**



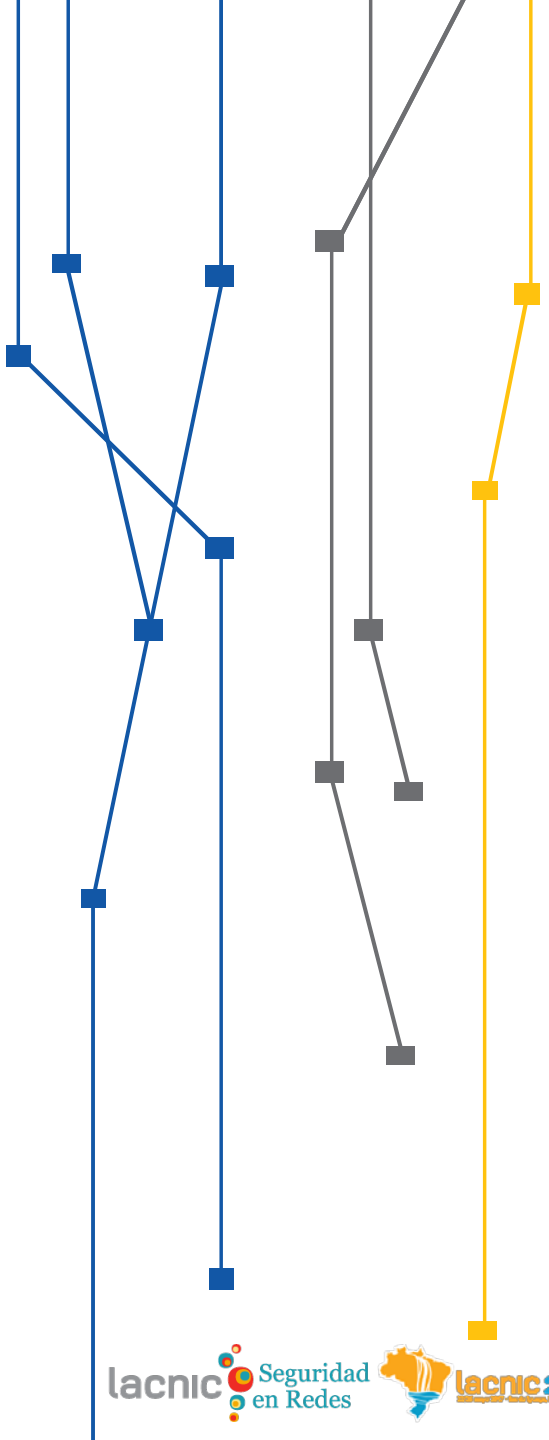
Motivation

Corporate security team and CSIRT is the same thing?



Motivation

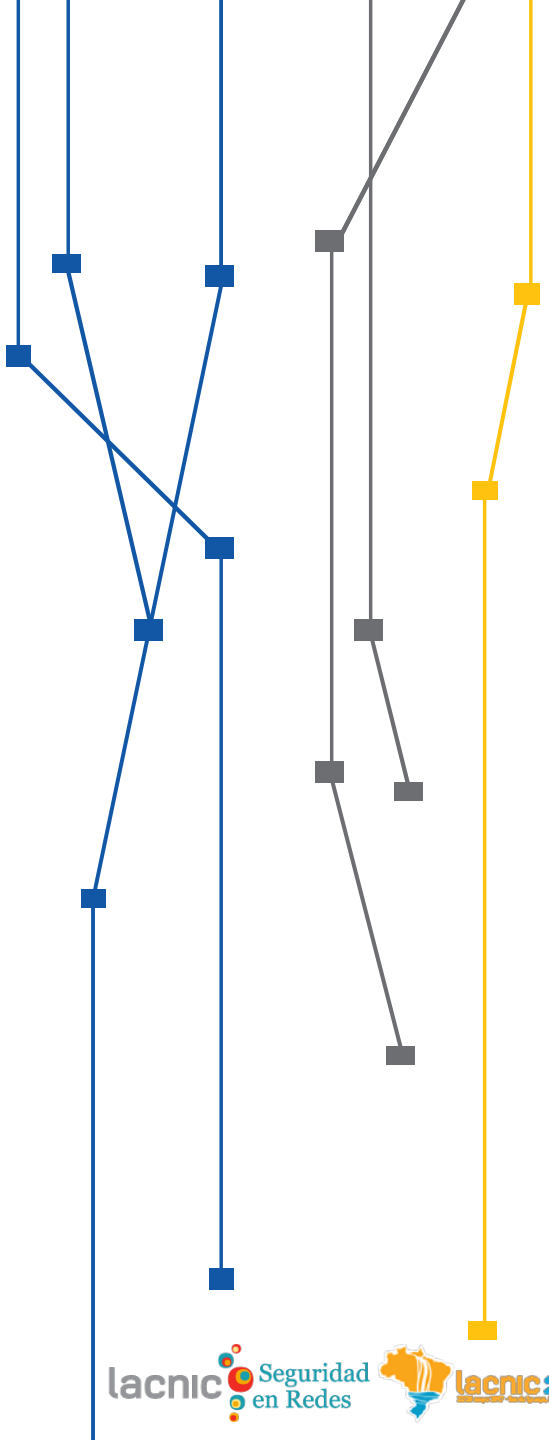
Security overview	Security incidents and critical vulnerabilities grew last years.
Security	Need to increase InfoSec capability in Brazilian
PROJECT	**CSIRTs in RNP Customers**
Brazilian NREN	especially for organizations that are part of Federal Public Administration
Incident handling focus	Corporate security team ≠ CSIRT



Goals

CSIRTs in RNP Customers Project

Template of CSIRT	Create a default and generic template to CSIRT establishment, applicable to Brazilian NREN environment.
Incident	Define a security incident management template, with process and procedures to all steps of incident
PROJECT	**CSIRTs in RNP Customers**
Guide	establishment of new CSIRTs.
Interaction	Promote interaction between new and existing CSIRT teams.



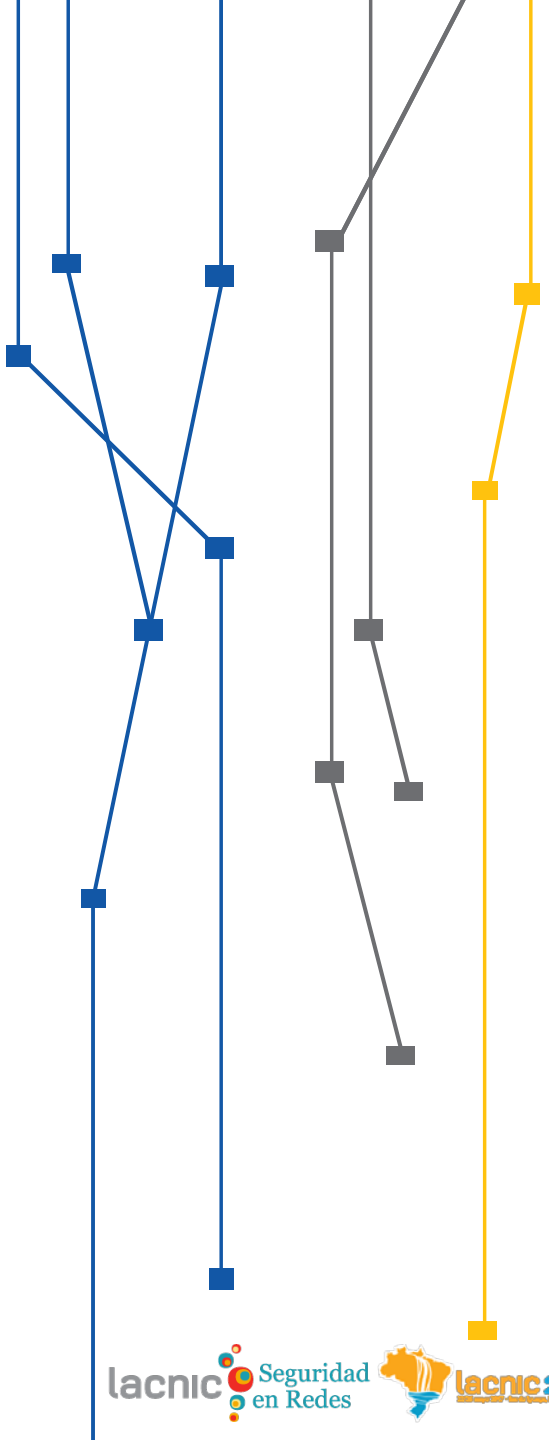
Technical Background

Standards

ABNT ISO/IEC 27002:2013

Guidelines of Security Incident Management.

- **Procedures and responsibilities;**
- **Security Information Events evaluation;**
- **Security Information Incidents response;**
- **Evidence collection.**

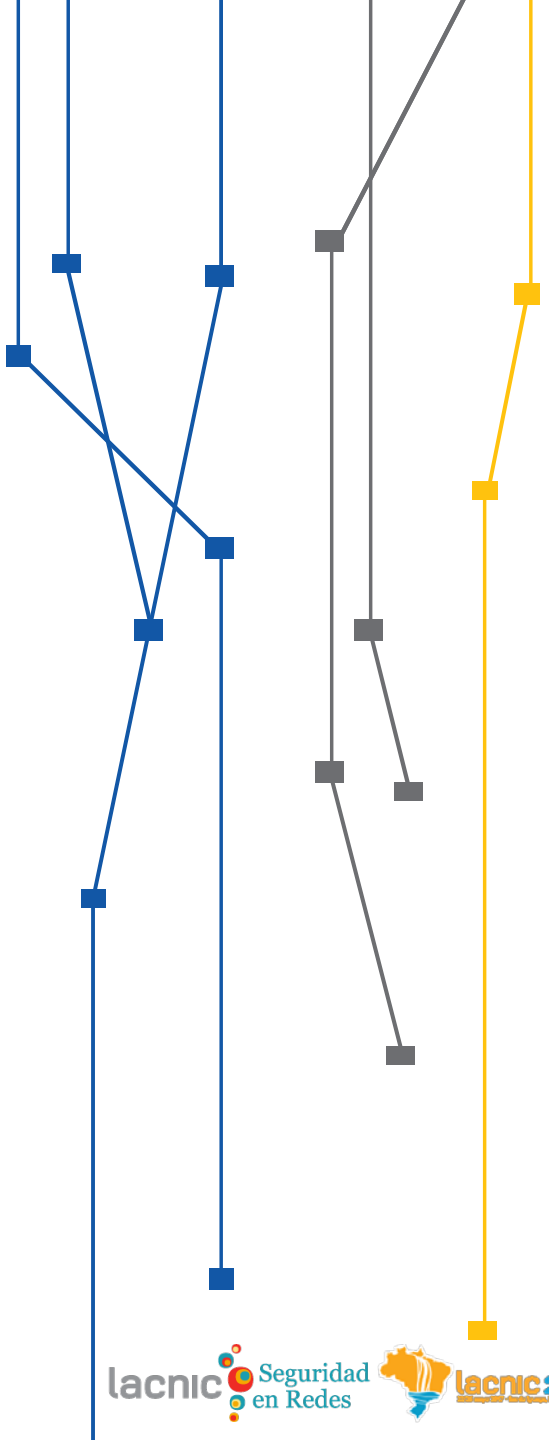


Technical Background

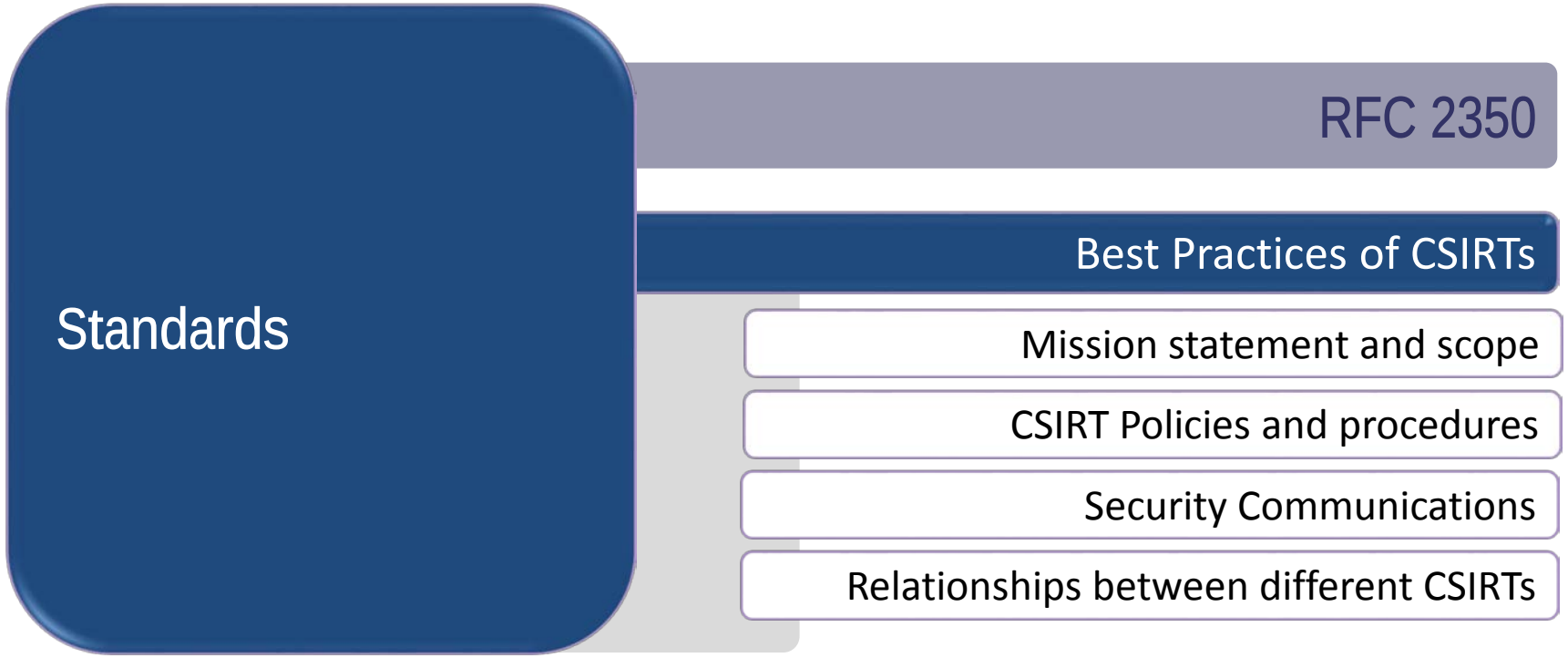
Standards

Normative Instruction GSI/PR Nº1:2008

Complementary Standard nº 05/IN01/DSIC/GSIPR	Disciplines creation of new CSIRT teams in Brazilian Federal Public Administration departments and entities.
Complementary Standard nº 08/IN01/DSIC/GSIPR	Establishes guidelines for Incident Management in Brazilian Federal Public Administration departments and entities.



Technical Background

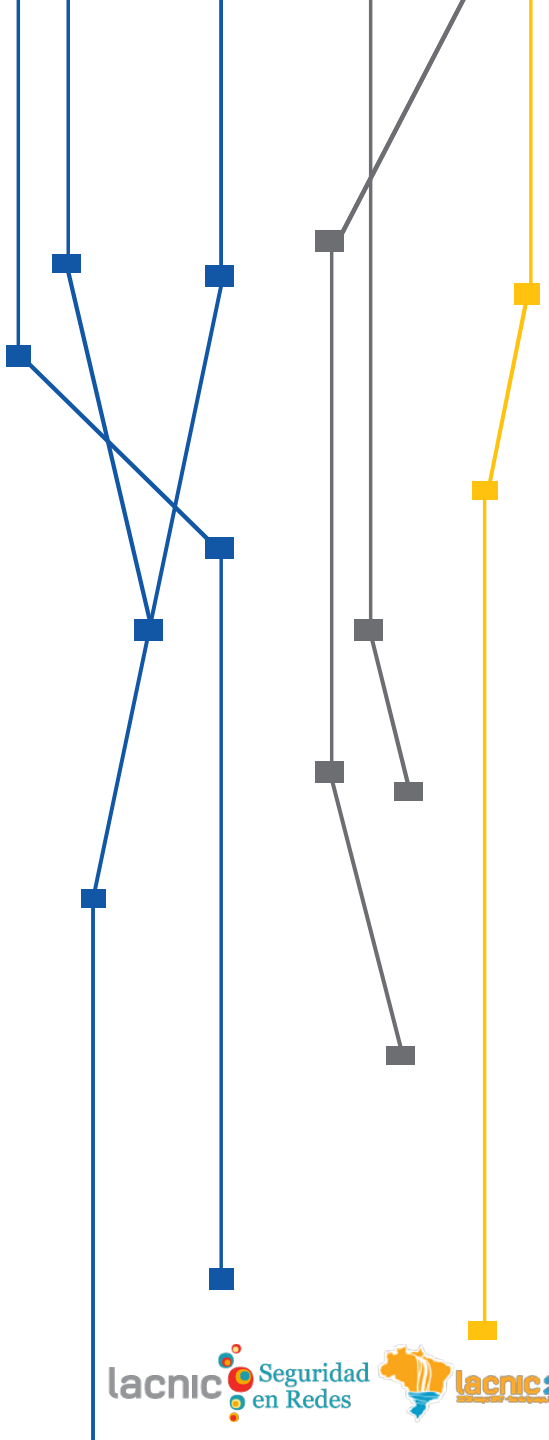


Technical Background

Standards

ABNT ISO/IEC 27035:2016

Security Incident Management guideline to external organizations who provides Information security incident management services.

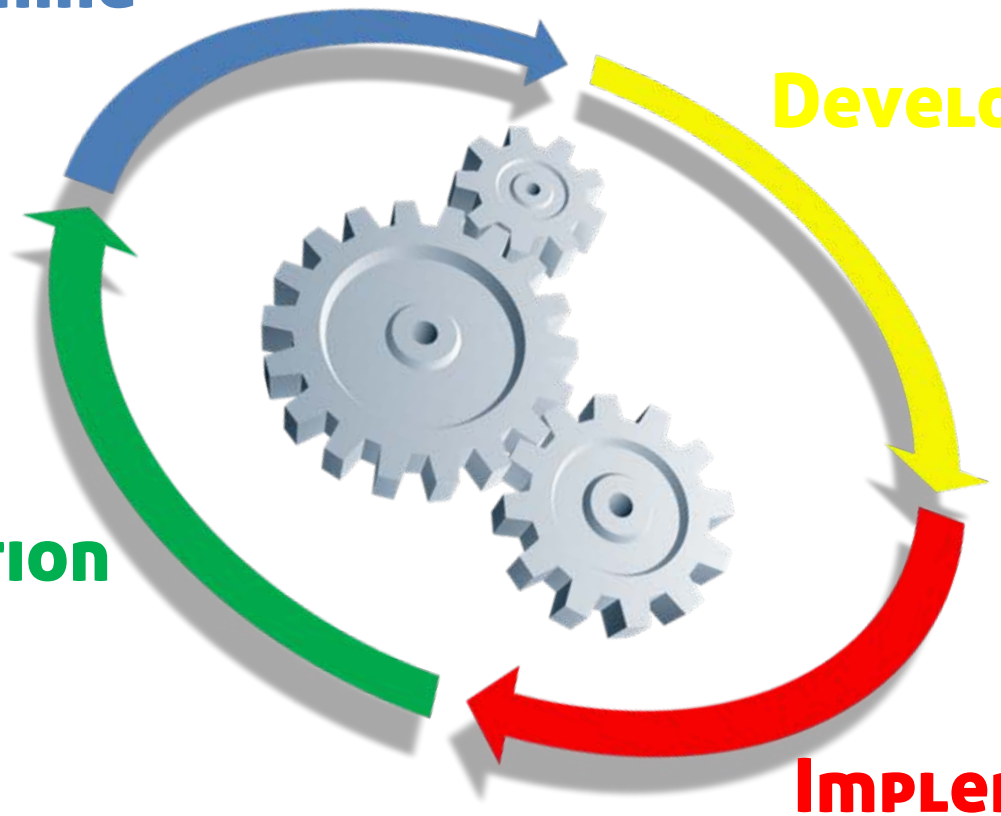


Where to start?

Methodology

Planning

Development



Operation

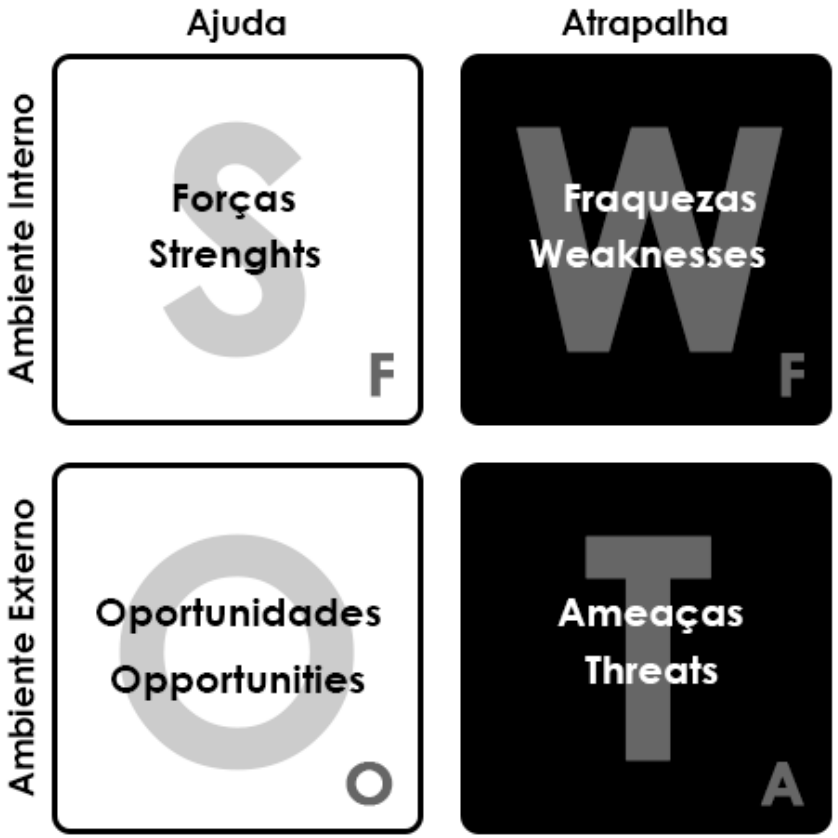
Implementation

Step 1: Planning

SWOT Analysis

Methodology used to analyze internal and external environment of an organization.

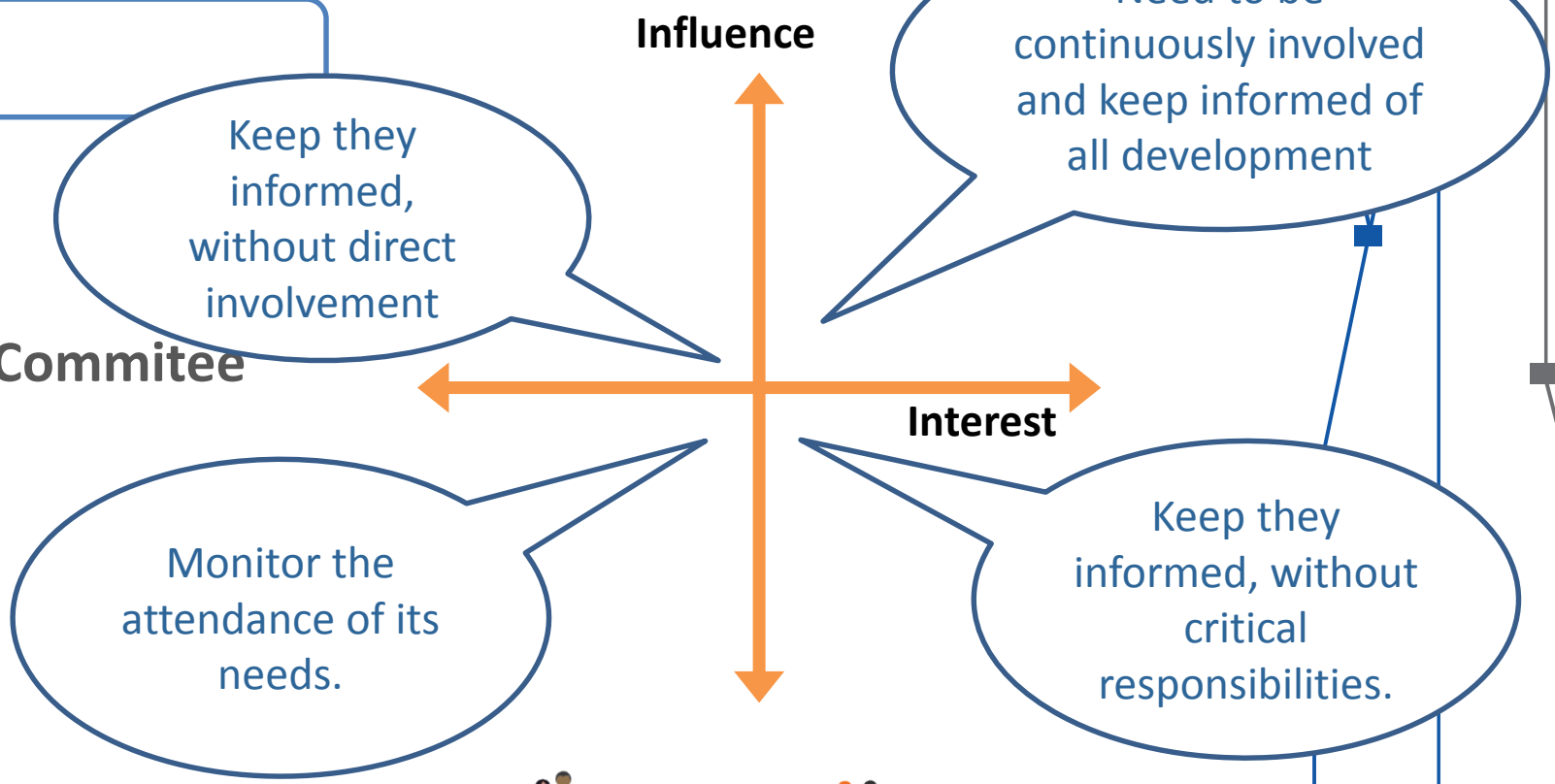
Data analysis with strategically positioning goal of an organization.



Step 1: Planning

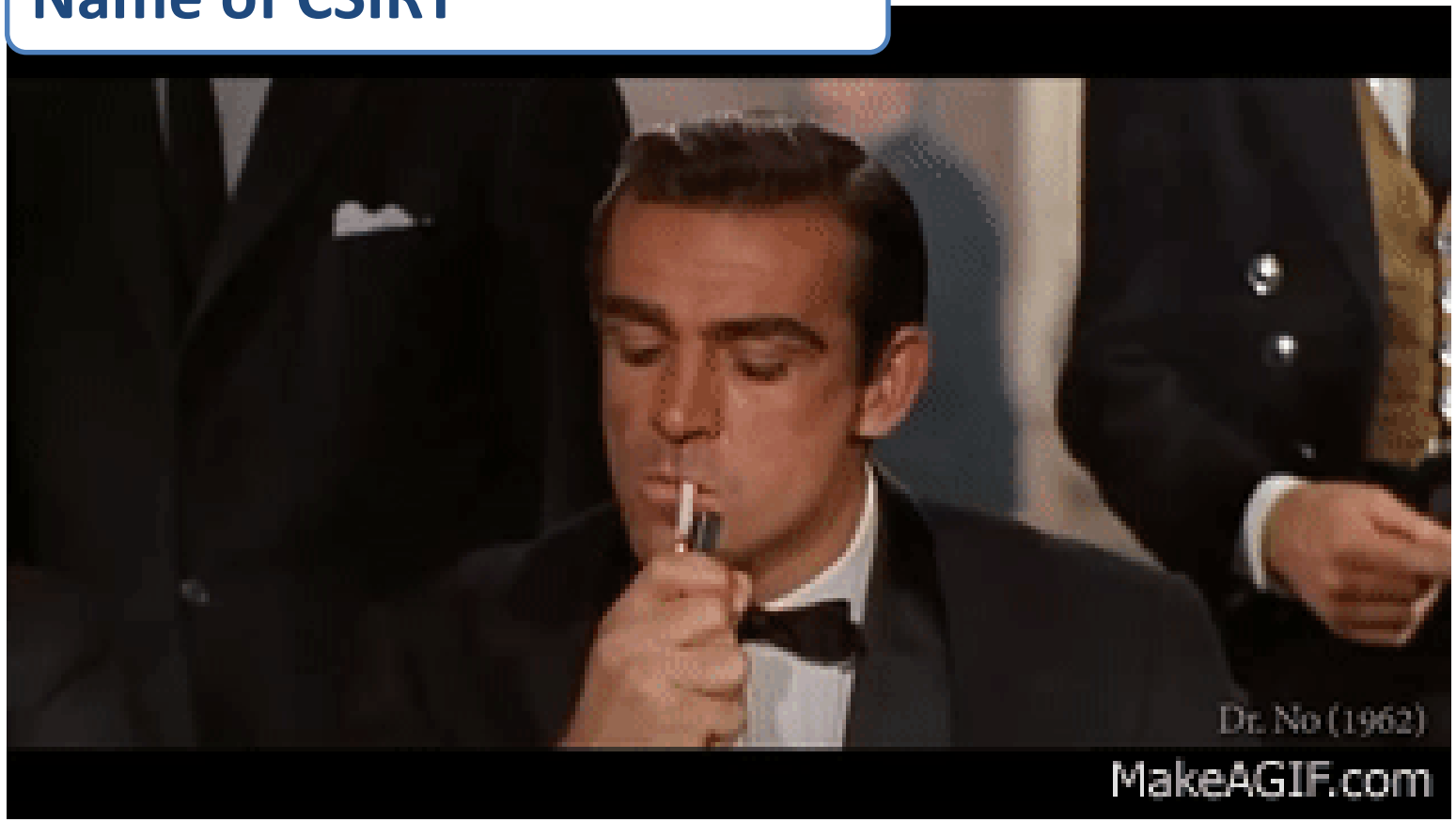
Stakeholders

- Project team
- Board of directors
- InfoSec Management Commitee
- Legal team
- Heritage sector
- IT Team
- Employees
- Students



Step 2: Development

Name of CSIRT



Step 2: Development

Mission

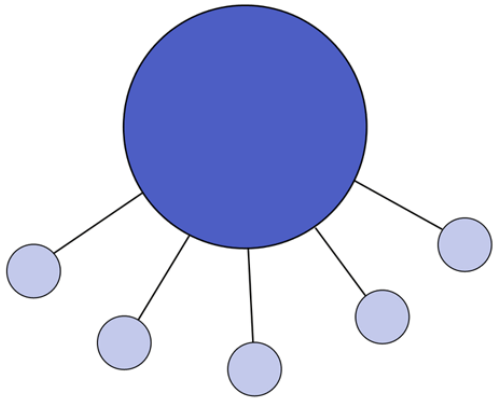
Constituency

Vision

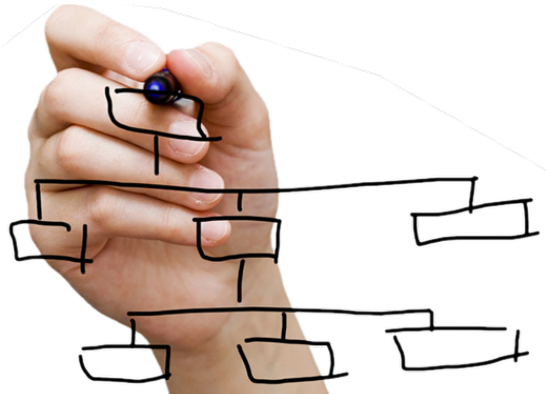
Services

Step 2: Development

Organizational Model



Organizational Structure



Authority

Step 3: Implementation

1) Infrastructure

2) People Management

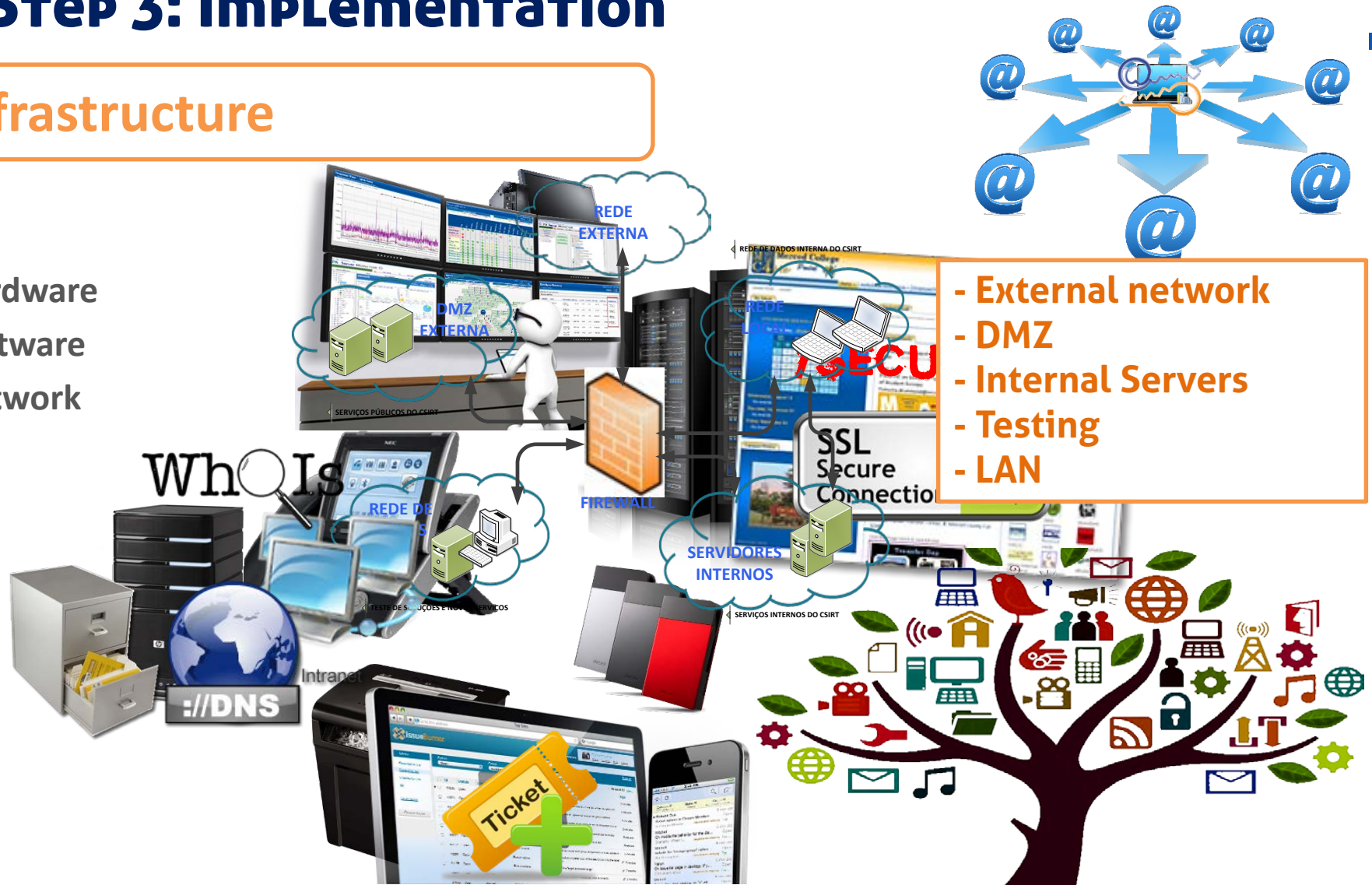
3) Funding

4) Policies and procedures

Step 3: Implementation

Infrastructure

- Hardware
- Software
- Network



- External network
- DMZ
- Internal Servers
- Testing
- LAN

Step 3: Implementation

People Management

Hiring

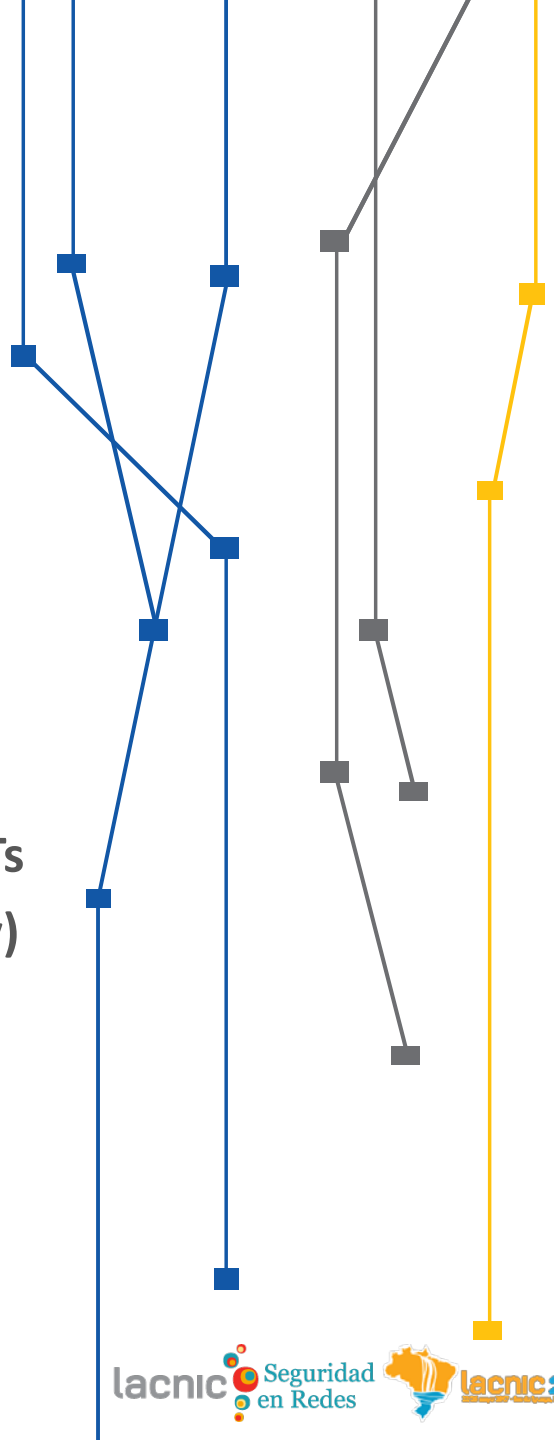
- Curriculum analysis
- Job interview
- Contract details
  * Career path
  * Workload (8x5? 24x7? Weekends?)
- Professional ethic

Firing

- Delete user/e-mail account
- Notice to organization

Professional development

- Follow up / coaching
- Events
  * CERT.br Brazilian Forum of CSIRTs
  * SBSeg (Security Brazilian Society)
  * Security Leaders
  * LACNIC / LACSEC
  * FIRST Technical Colloquium



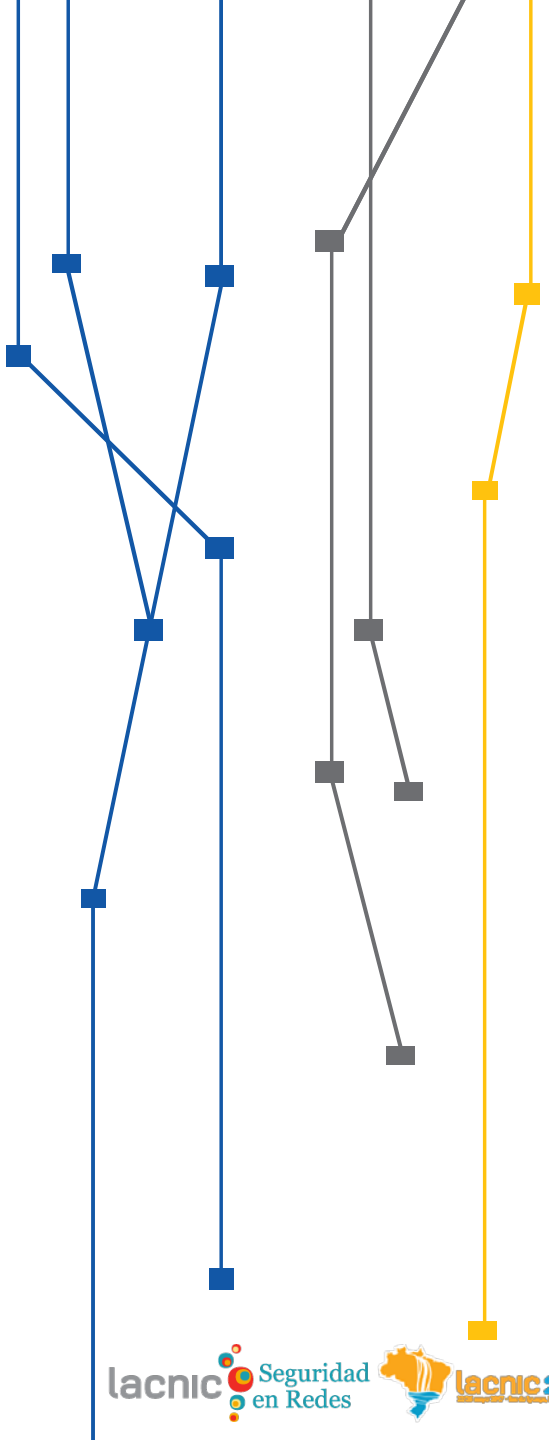
Step 3: Implementation

Funding

- Specific budget to CSIRT
- Partnership with other CSIRTs
- Sale of services to customers
- Submit projects to Research Funding Organizations

Policies and Procedures

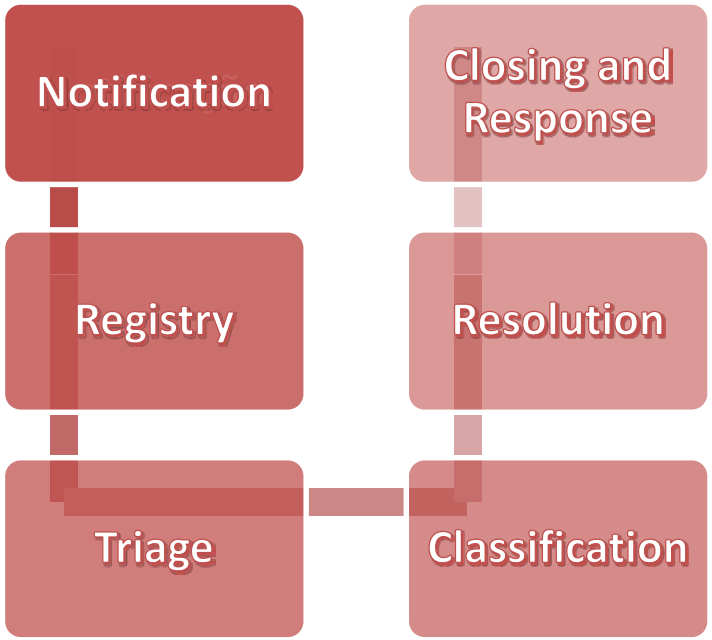
- Information handling / Information classification
- Resources usage policies
- Password policies
- Communication Plan
- Security Awareness Plan



Step 3: Implementation

Incident Management Plan

Six main steps:



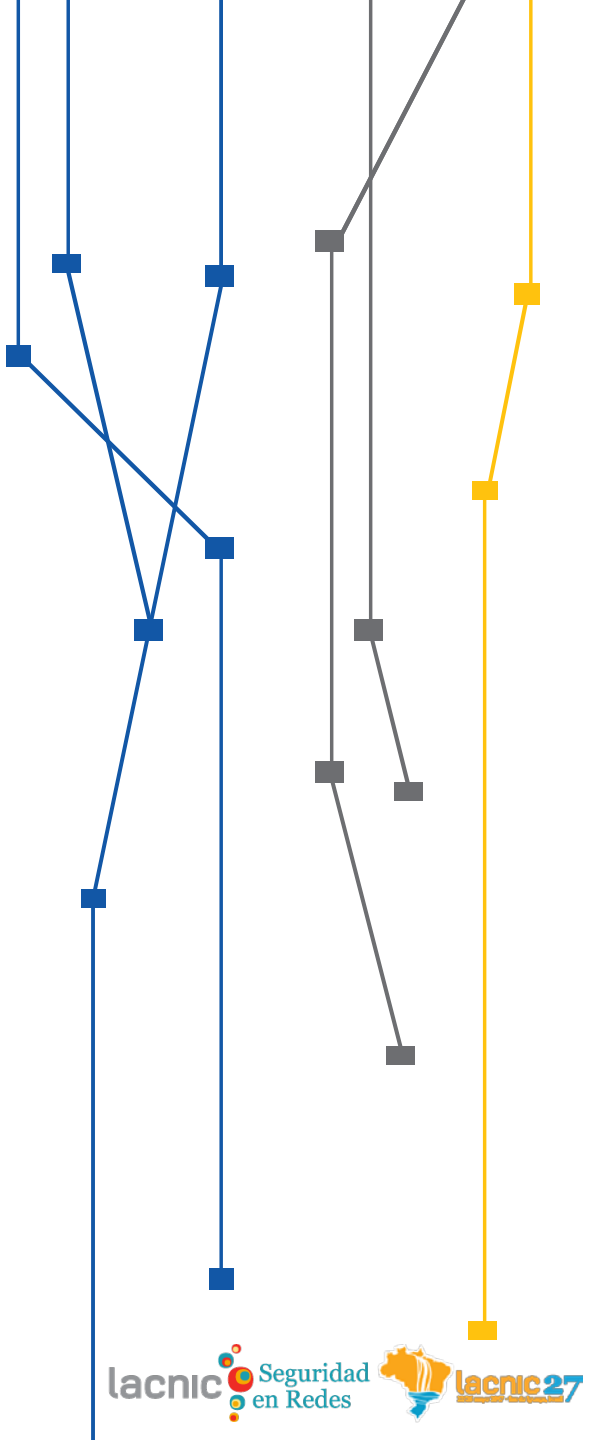
Step 3: Implementation

Incident Management Plan

Six main steps:

Notification

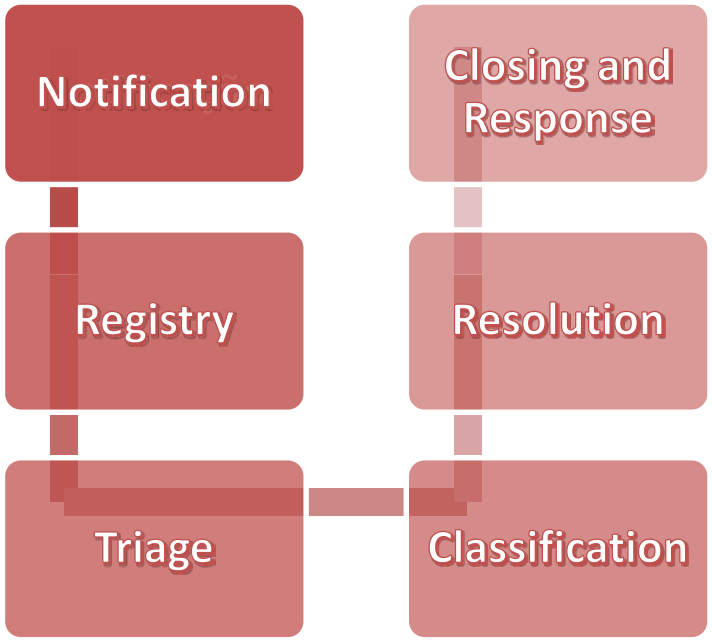
- Security incident notification channels
  - Communication systems;
  - Malicious activity detection;
- Security incident notification elements
  - Incident description
  - IP source / destination
  - Ports / protocols / compromised services
  - Date and time (with correct GMT)



Step 3: Implementation

Incident Management Plan

Six main steps:



Step 4: Operation

Formalization

- CSIRT formalization document template

Disclosure

- E-mail marketing
- Website
- Awareness lectures

Analysis

- Statistics
  * Incidents by time / category
  * More used protocols
  * IP address involved
- Indicators
  * Incidents closed in/out time
  * Incidents closed in certain period
  * Time spent to close incidents

Step 4: Operation

CSIRT formalization document sample

[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:

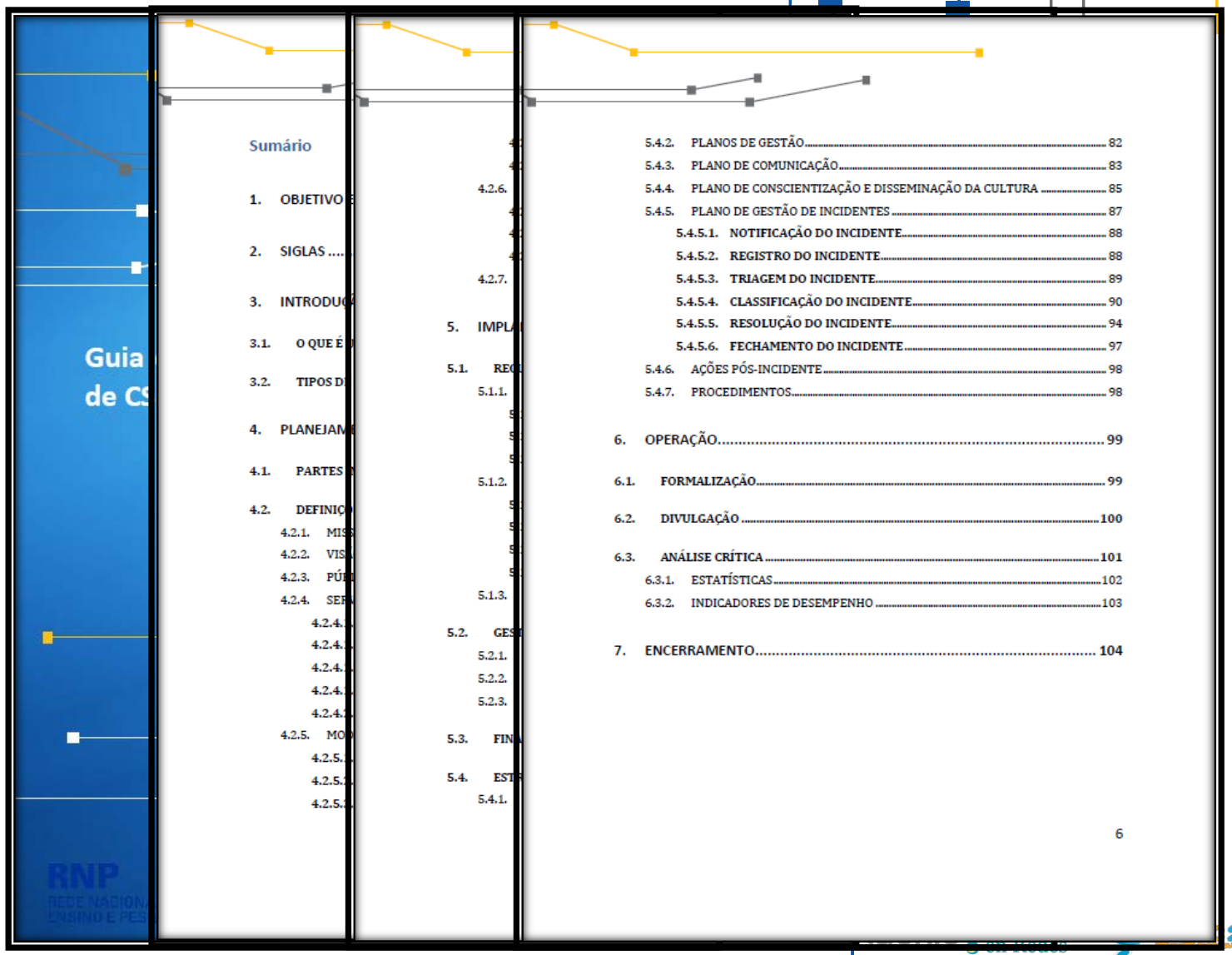
º - Instituir a Equipe de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – NOME DO CSIRT, na rede computacional da NOME DA INSTITUIÇÃO, em observância à determinação lecida pelo artigo Nº da Política de Segurança da Informação e Comunicações, conforme definido a seguir.

CAPITULO I – DA MISSÃO

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

Results

– Establishment CSIRTs in Brazilian NREN Best Practices Guide

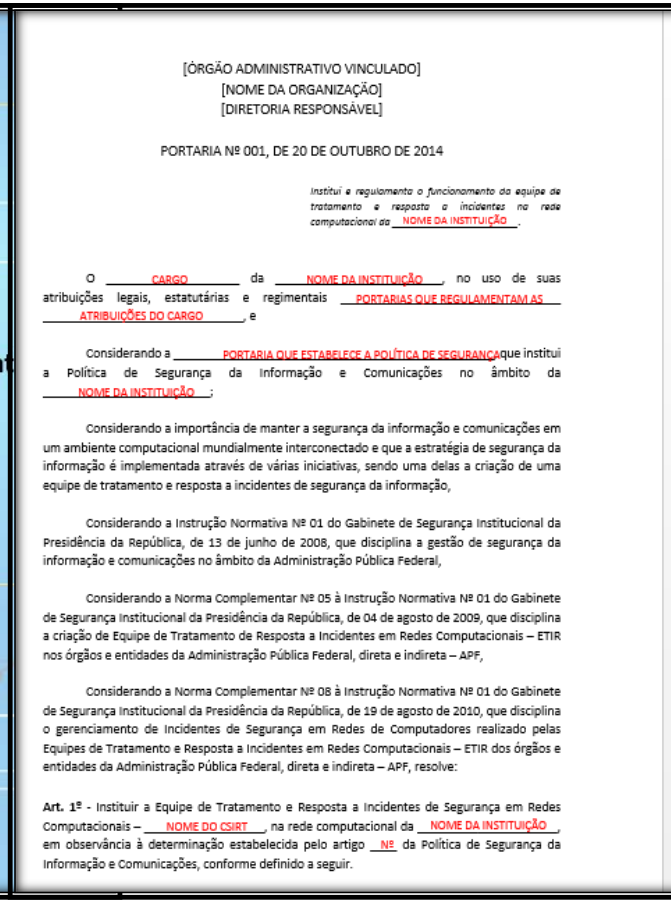


Results

– Establishment CSIRT Checklist

Results

– Documentation template



[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 implementada 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 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 Incidentes 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:

Art. 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 estabelecida pelo artigo Nº da Política de Segurança da Informação e Comunicações, conforme definido a seguir.

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.

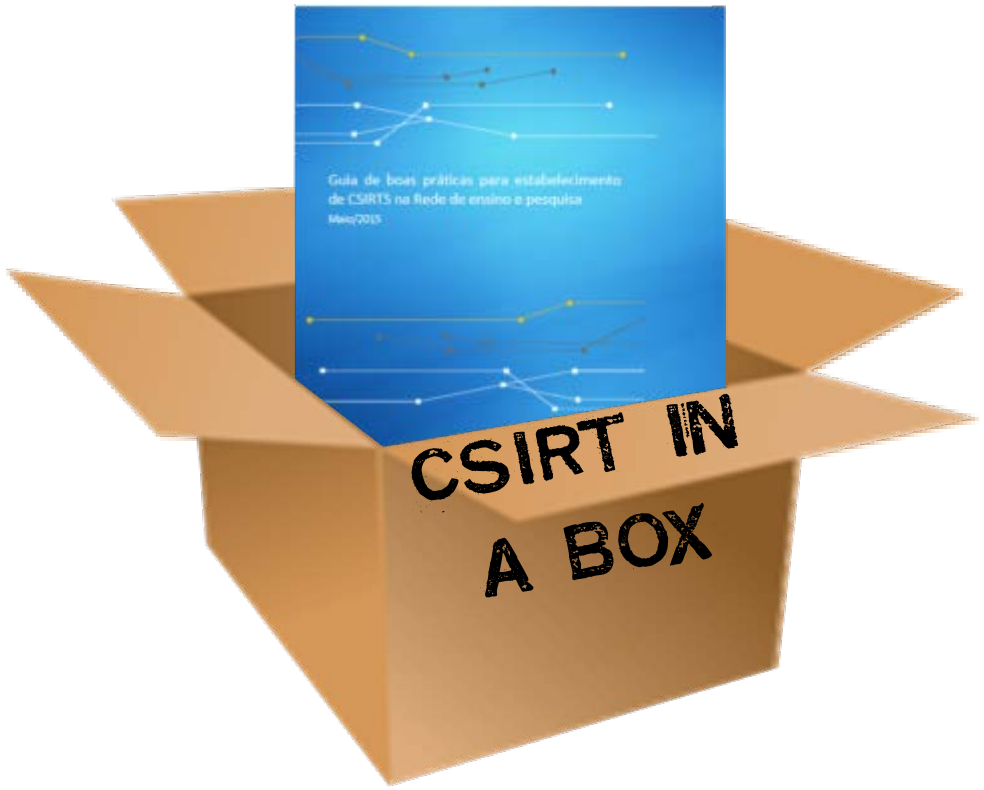
Results


Guia de boas práticas para estabelecimento
de CSIRTS na Rede de ensino e pesquisa
Maio/2015
RNP

Results


Guia de boas práticas para estabelecimento de CSIRTS na Rede de ensino e pesquisa
Maio/2015
RNP

Results


Guia de boas práticas para estabelecimento de CSIRTS na Rede de ensino e pesquisa
Maio/2015
CSIRT IN A BOX

Cases

UFBA

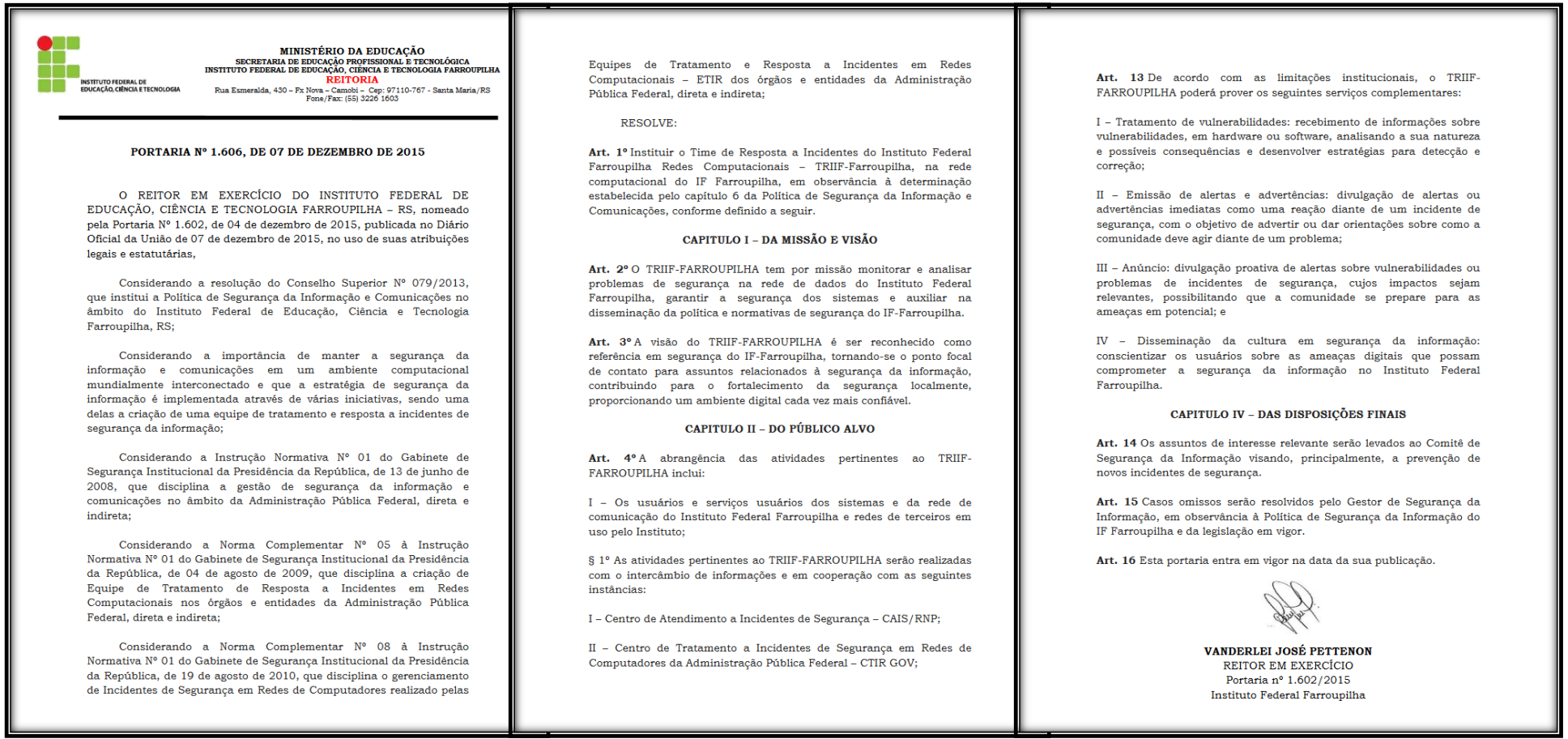
Salvador/BA

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
FARROUPILHA

Santa Maria/RS

Cases

TRIIF – Incident Response Team of Instituto Federal Farroupilha



MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FARROUPILHA
REITORIA
Rua Esmeralda, 430 – Fx Nova – Camobi – Cep: 97110-767 - Santa Maria/RS
Fone/Fax: (55) 3226 1603

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

PORTARIA Nº 1.606, DE 07 DE DEZEMBRO DE 2015

O REITOR EM EXERCÍCIO DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA FARROUPILHA – RS, nomeado pela Portaria Nº 1.602, de 04 de dezembro de 2015, publicada no Diário Oficial da União de 07 de dezembro de 2015, no uso de suas atribuições legais e estatutárias,

Considerando a resolução do Conselho Superior Nº 079/2013, que institui a Política de Segurança da Informação e Comunicações no âmbito do Instituto Federal de Educação, Ciência e Tecnologia Farroupilha, RS;

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 implementada 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, direta e indireta;

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 de Resposta a Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal, direta e indireta;

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 Incidentes 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;

RESOLVE:

Art. 1º Instituir o Time de Resposta a Incidentes do Instituto Federal Farroupilha Redes Computacionais – TRIIF-Farroupilha, na rede computacional do IF Farroupilha, em observância à determinação estabelecida pelo capítulo 6 da Política de Segurança da Informação e Comunicações, conforme definido a seguir.

CAPITULO I – DA MISSÃO E VISÃO

Art. 2º O TRIIF-FARROUPILHA tem por missão monitorar e analisar problemas de segurança na rede de dados do Instituto Federal Farroupilha, garantir a segurança dos sistemas e auxiliar na disseminação da política e normativas de segurança do IF-Farroupilha.

Art. 3º A visão do TRIIF-FARROUPILHA é ser reconhecido como referência em segurança do IF-Farroupilha, tornando-se o ponto focal de contato para assuntos relacionados à segurança da informação, contribuindo para o fortalecimento da segurança localmente, proporcionando um ambiente digital cada vez mais confiável.

CAPITULO II – DO PÚBLICO ALVO

Art. 4º A abrangência das atividades pertinentes ao TRIIF-FARROUPILHA inclui:

I – Os usuários e serviços usuários dos sistemas e da rede de comunicação do Instituto Federal Farroupilha e redes de terceiros em uso pelo Instituto;

§ 1º As atividades pertinentes ao TRIIF-FARROUPILHA 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;

Art. 13 De acordo com as limitações institucionais, o TRIIF-FARROUPILHA poderá prover os seguintes serviços complementares:

I – Tratamento de vulnerabilidades: recebimento de informações sobre vulnerabilidades, em hardware ou software, analisando a sua natureza e possíveis consequências e desenvolver estratégias para detecção e correção;

II – Emissão de alertas e advertências: divulgação de alertas ou advertências imediatas como uma reação diante de um incidente de segurança, com o objetivo de advertir ou dar orientações sobre como a comunidade deve agir diante de um problema;

III – Anúncio: divulgação proativa de alertas sobre vulnerabilidades ou problemas de incidentes de segurança, cujos impactos sejam relevantes, possibilitando que a comunidade se prepare para as ameaças em potencial; e

IV – Disseminação da cultura em segurança da informação: conscientizar os usuários sobre as ameaças digitais que possam comprometer a segurança da informação no Instituto Federal Farroupilha.

CAPITULO IV – DAS DISPOSIÇÕES FINAIS

Art. 14 Os assuntos de interesse relevante serão levados ao Comitê de Segurança da Informação visando, principalmente, a prevenção de novos incidentes de segurança.

Art. 15 Casos omissos serão resolvidos pelo Gestor de Segurança da Informação, em observância à Política de Segurança da Informação do IF Farroupilha e da legislação em vigor.

Art. 16 Esta portaria entra em vigor na data da sua publicação.

VANDERLEI JOSÉ PETTENON
REITOR EM EXERCÍCIO
Portaria nº 1.602/2015
Instituto Federal Farroupilha

lacnic Seguridad en Redes lacnic27

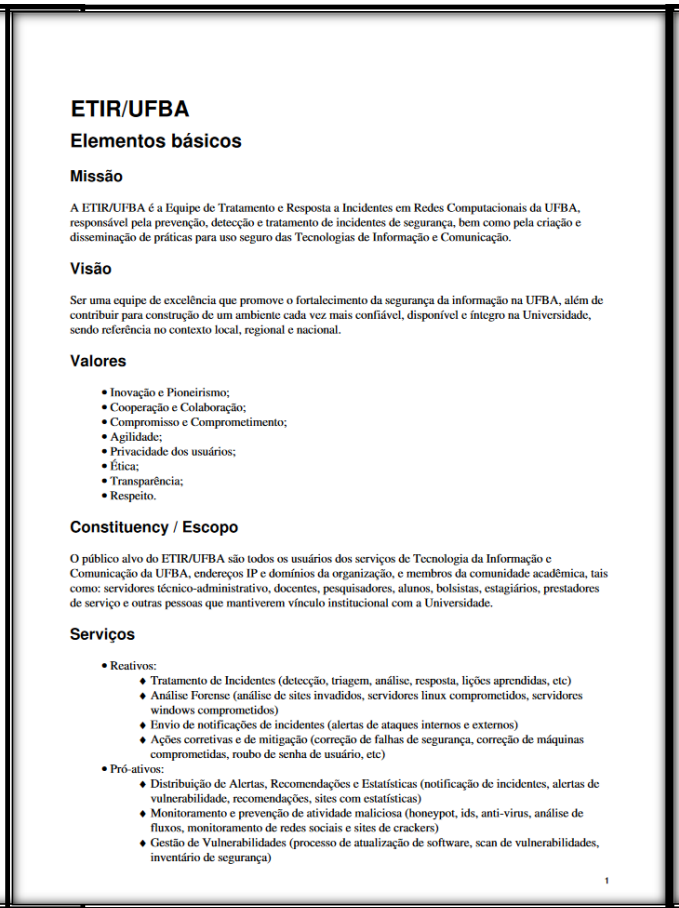
Cases

TRIIF – Incident Response Team of Instituto Federal Farroupilha

http://triif.iffarroupilha.edu.br

Cases

UFBA – Federal University of Bahia



ETIR/UFBA

Elementos básicos

Missão

A ETIR/UFBA é a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais da UFBA, responsável pela prevenção, detecção e tratamento de incidentes de segurança, bem como pela criação e disseminação de práticas para uso seguro das Tecnologias de Informação e Comunicação.

Visão

Ser uma equipe de excelência que promove o fortalecimento da segurança da informação na UFBA, além de contribuir para construção de um ambiente cada vez mais confiável, disponível e íntegro na Universidade, sendo referência no contexto local, regional e nacional.

Valores

- Inovação e Pioneirismo;
- Cooperação e Colaboração;
- Compromisso e Comprometimento;
- Agilidade;
- Privacidade dos usuários;
- Ética;
- Transparência;
- Respeito.

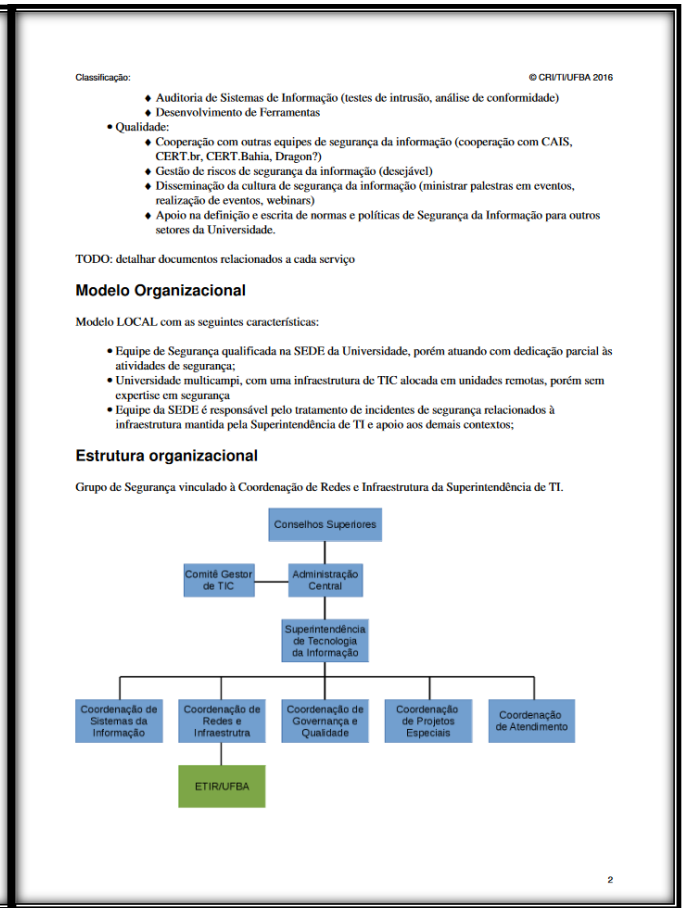
Constituency / Escopo

O público alvo do ETIR/UFBA são todos os usuários dos serviços de Tecnologia da Informação e Comunicação da UFBA, endereços IP e domínios da organização, e membros da comunidade acadêmica, tais como: servidores técnico-administrativo, docentes, pesquisadores, alunos, bolsistas, estagiários, prestadores de serviço e outras pessoas que mantiverem vínculo institucional com a Universidade.

Serviços

- Reativos:
  - Tratamento de Incidentes (detecção, triagem, análise, resposta, lições aprendidas, etc)
  - Análise Forense (análise de sites invadidos, servidores linux comprometidos, servidores windows comprometidos)
  - Envio de notificações de incidentes (alertas de ataques internos e externos)
  - Ações corretivas e de mitigação (correção de falhas de segurança, correção de máquinas comprometidas, roubo de senha de usuário, etc)
- Pró-ativos:
  - Distribuição de Alertas, Recomendações e Estatísticas (notificação de incidentes, alertas de vulnerabilidade, recomendações, sites com estatísticas)
  - Monitoramento e prevenção de atividade maliciosa (honeypot, ids, anti-virus, análise de fluxos, monitoramento de redes sociais e sites de crackers)
  - Gestão de Vulnerabilidades (processo de atualização de software, scan de vulnerabilidades, inventário de segurança)

1



Classificação: © CRI/TI/UFBA 2016

  - Auditoria de Sistemas de Informação (testes de intrusão, análise de conformidade)
  - Desenvolvimento de Ferramentas
- Qualidade:
  - Cooperação com outras equipes de segurança da informação (cooperação com CAIS, CERT.br, CERT.Bahia, Dragon?)
  - Gestão de riscos de segurança da informação (desejável)
  - Disseminação da cultura de segurança da informação (ministrar palestras em eventos, realização de eventos, webinars)
  - Apoio na definição e escrita de normas e políticas de Segurança da Informação para outros setores da Universidade.

TODO: detalhar documentos relacionados a cada serviço

Modelo Organizacional

Modelo LOCAL com as seguintes características:

- Equipe de Segurança qualificada na SEDE da Universidade, porém atuando com dedicação parcial às atividades de segurança;
- Universidade multicampi, com uma infraestrutura de TIC alocada em unidades remotas, porém sem expertise em segurança
- Equipe da SEDE é responsável pelo tratamento de incidentes de segurança relacionados à infraestrutura mantida pela Superintendência de TI e apoio aos demais contextos;

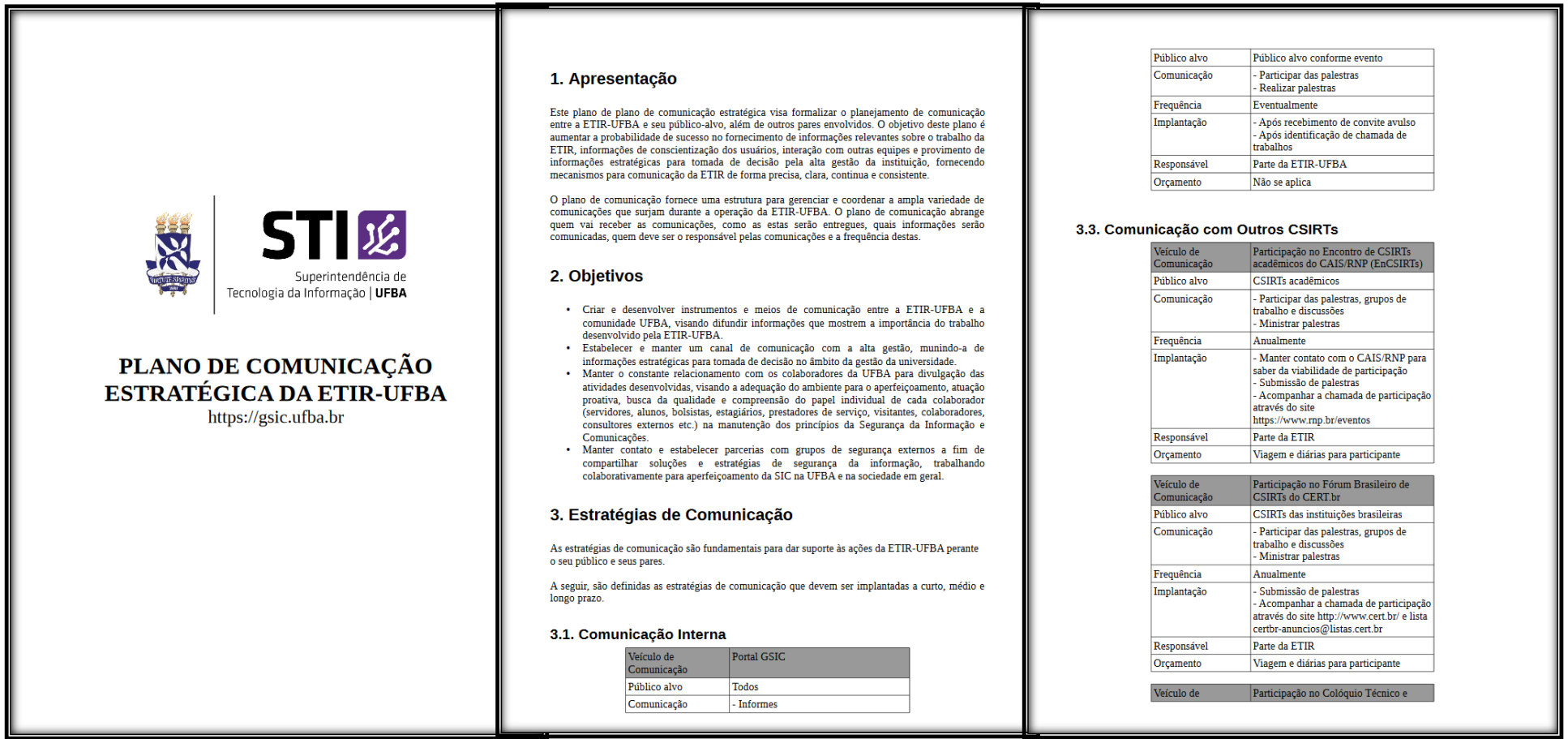
Estrutura organizacional

Grupo de Segurança vinculado à Coordenação de Redes e Infraestrutura da Superintendência de TI.

2

Cases

UFBA – Federal University of Bahia



STI
Superintendência de Tecnologia da Informação | UFBA

PLANO DE COMUNICAÇÃO ESTRATÉGICA DA ETIR-UFBA

https://gsic.ufba.br

1. Apresentação

Este plano de plano de comunicação estratégica visa formalizar o planejamento de comunicação entre a ETIR-UFBA e seu público-alvo, além de outros pares envolvidos. O objetivo deste plano é aumentar a probabilidade de sucesso no fornecimento de informações relevantes sobre o trabalho da ETIR, informações de conscientização dos usuários, interação com outras equipes e provimento de informações estratégicas para tomada de decisão pela alta gestão da instituição, fornecendo mecanismos para comunicação da ETIR de forma precisa, clara, continua e consistente.

O plano de comunicação fornece uma estrutura para gerenciar e coordenar a ampla variedade de comunicações que surjam durante a operação da ETIR-UFBA. O plano de comunicação abrange quem vai receber as comunicações, como as estas serão entregues, quais informações serão comunicadas, quem deve ser o responsável pelas comunicações e a frequência destas.

2. Objetivos

- Criar e desenvolver instrumentos e meios de comunicação entre a ETIR-UFBA e a comunidade UFBA, visando difundir informações que mostrem a importância do trabalho desenvolvido pela ETIR-UFBA.
- Estabelecer e manter um canal de comunicação com a alta gestão, munindo-a de informações estratégicas para tomada de decisão no âmbito da gestão da universidade.
- Manter o constante relacionamento com os colaboradores da UFBA para divulgação das atividades desenvolvidas, visando a adequação do ambiente para o aperfeiçoamento, atuação proativa, busca da qualidade e compreensão do papel individual de cada colaborador (servidores, alunos, bolsistas, estagiários, prestadores de serviço, visitantes, colaboradores, consultores externos etc.) na manutenção dos princípios da Segurança da Informação e Comunicações.
- Manter contato e estabelecer parcerias com grupos de segurança externos a fim de compartilhar soluções e estratégias de segurança da informação, trabalhando colaborativamente para aperfeiçoamento da SIC na UFBA e na sociedade em geral.

3. Estratégias de Comunicação

As estratégias de comunicação são fundamentais para dar suporte às ações da ETIR-UFBA perante o seu público e seus pares.

A seguir, são definidas as estratégias de comunicação que devem ser implantadas a curto, médio e longo prazo.

3.1. Comunicação Interna

Veículo de Comunicação	Portal GSIC
Público alvo	Todos
Comunicação	- Informes
Público alvo	Público alvo conforme evento
Comunicação	- Participar das palestras - Realizar palestras
Frequência	Eventualmente
Implantação	- Após recebimento de convite avulso - Após identificação de chamada de trabalhos
Responsável	Parte da ETIR-UFBA
Orçamento	Não se aplica

3.3. Comunicação com Outros CSIRTs

Veículo de Comunicação	Participação no Encontro de CSIRTs acadêmicos do CAIS/RNP (EnCSIRTs)
Público alvo	CSIRTs acadêmicos
Comunicação	- Participar das palestras, grupos de trabalho e discussões - Ministrar palestras
Frequência	Anualmente
Implantação	- Manter contato com o CAIS/RNP para saber da viabilidade de participação - Submissão de palestras - Acompanhar a chamada de participação através do site https://www.rnp.br/eventos
Responsável	Parte da ETIR
Orçamento	Viagem e diárias para participante

Veículo de Comunicação	Participação no Fórum Brasileiro de CSIRTs do CERT.br
Público alvo	CSIRTs das instituições brasileiras
Comunicação	- Participar das palestras, grupos de trabalho e discussões - Ministrar palestras
Frequência	Anualmente
Implantação	- Submissão de palestras - Acompanhar a chamada de participação através do site http://www.cert.br/ e lista certbr-anuncios@listas.cert.br
Responsável	Parte da ETIR
Orçamento	Viagem e diárias para participante

Veículo de	Participação no Colóquio Técnico e

lacnic Seguridad en Redes lacnic27

Cases

UFBA – Federal University of Bahia

STI
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.

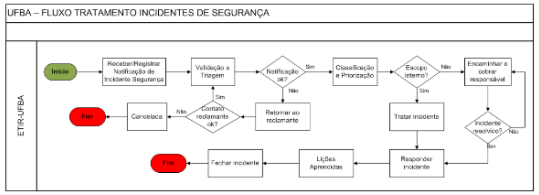


Fig. 1: Fluxo de Tratamento de Incidentes de Segurança da ETIR-UFBA

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.

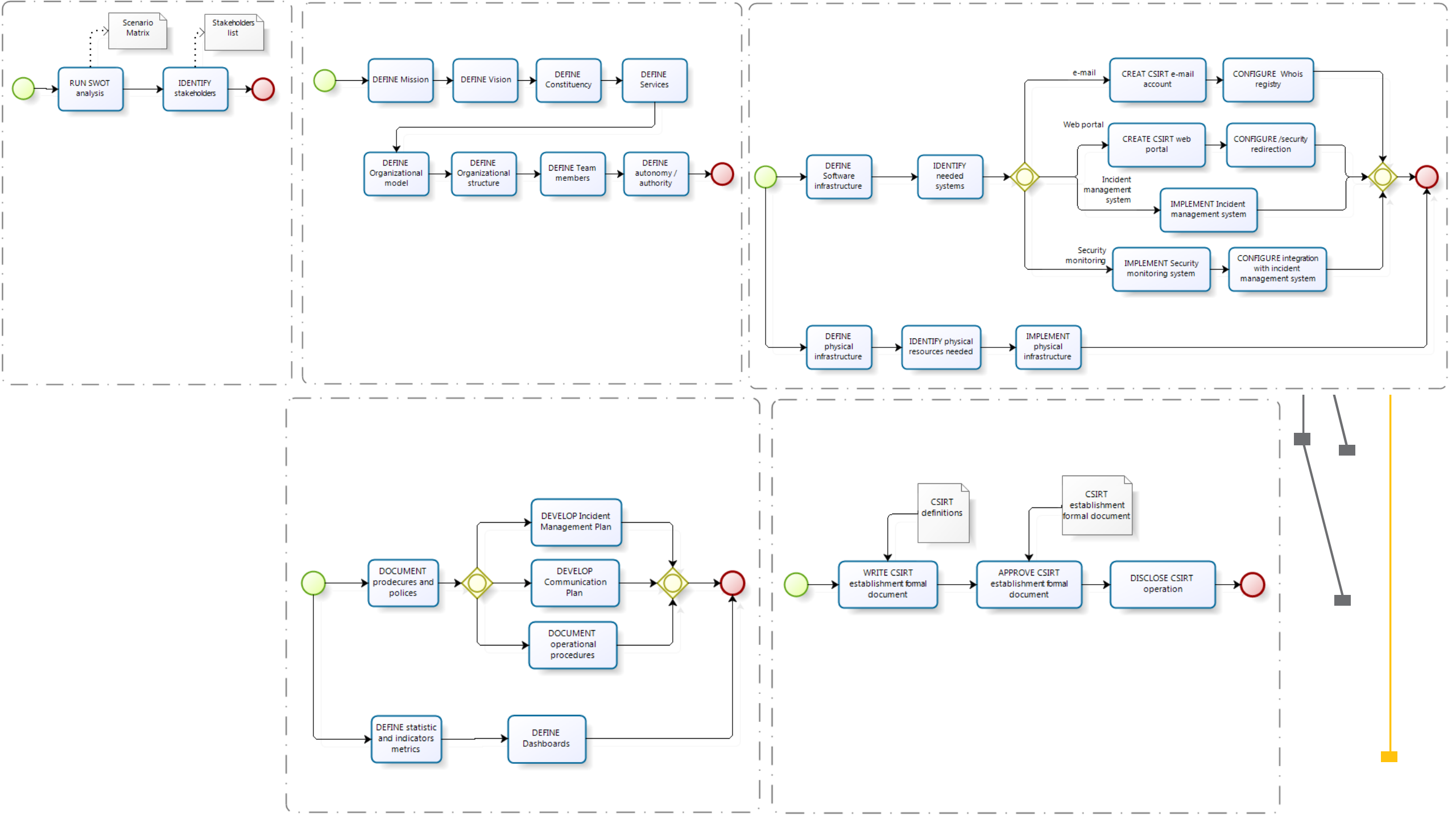
3.1.2 Envio de Notificações

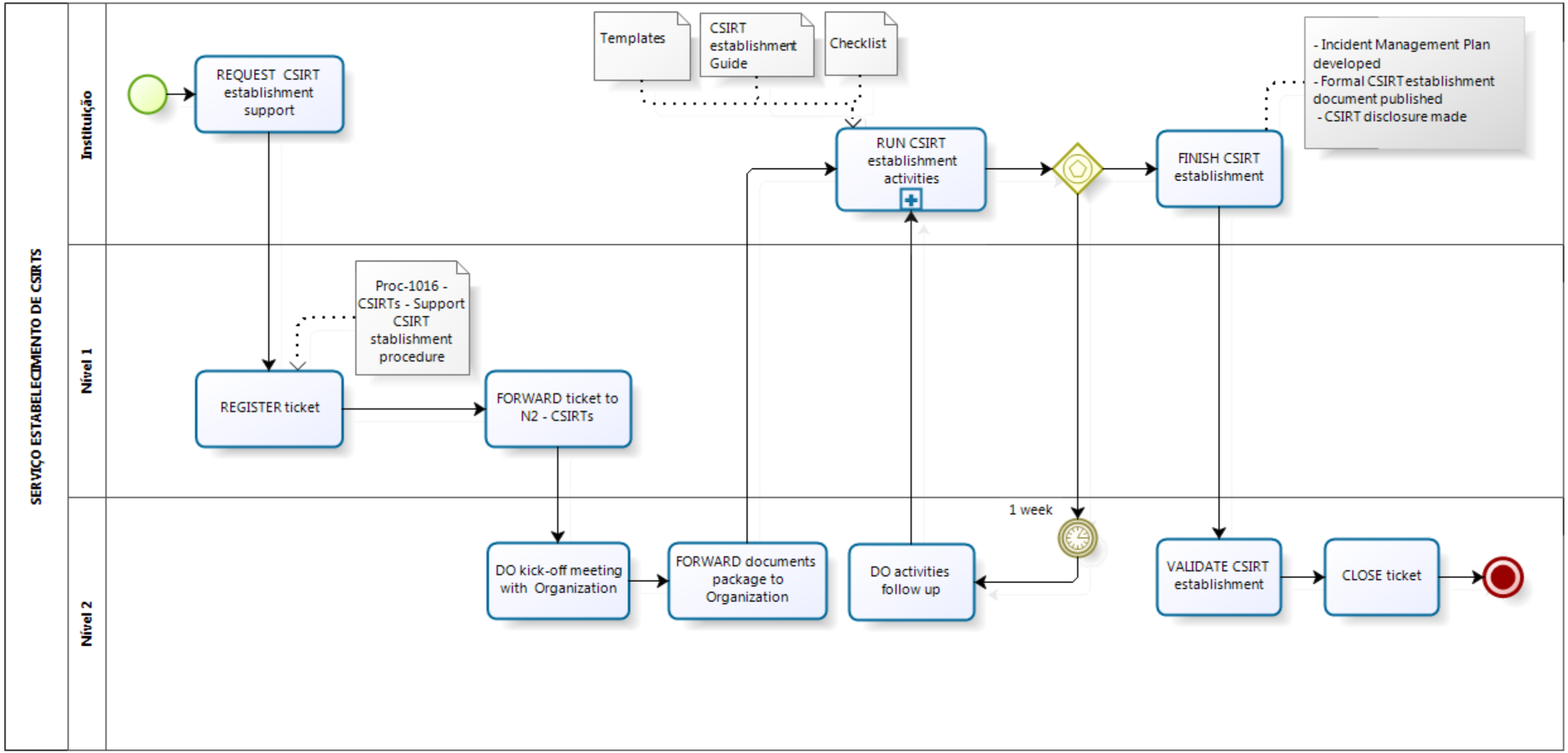
Os incidentes de segurança enviados pelo ETIR-UFBA para equipes ou órgãos internos ou externos devem conter um conjunto mínimo de informações que possibilite seu tratamento adequado pelo responsável. As notificações serão enviadas prioritariamente por e-mail, através da conta **etir@ufba.br**. Abaixo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


Scenario Matrix
Stakeholders list
RUN SWOT analysis
IDENTIFY stakeholders
DEFINE Mission
DEFINE Vision
DEFINE Constituency
DEFINE Services
DEFINE Organizational model
DEFINE Organizational structure
DEFINE Team members
DEFINE autonomy / authority
DEFINE Software infrastructure
IDENTIFY needed systems
e-mail
CREAT CSIRT e-mail account
CONFIGURE Whois registry
Web portal
CREATE CSIRT web portal
CONFIGURE /security redirection
Incident management system
IMPLEMENT Incident management system
Security monitoring
IMPLEMENT Security monitoring system
CONFIGURE integration with incident management system
DEFINE physical infrastructure
IDENTIFY physical resources needed
IMPLEMENT physical infrastructure
DOCUMENT prodecures and polices
DEVELOP Incident Management Plan
DEVELOP Communication Plan
DOCUMENT operational procedures
DEFINE statistic and indicators metrics
DEFINE Dashboards
CSIRT definitions
CSIRT establishment formal document
WRITE CSIRT establishment formal document
APPROVE CSIRT establishment formal document
DISCLOSE CSIRT operation



Thanks!

RNP – Brazilian Educational and Research Network

CAIS – RNP Incident Security Response Team

Rildo Souza

Security Analyst

rildo.souza@rnp.br

Yuri Alexandro

Security Analyst

yuri.ferreira@rnp.br

RNP

Ministério da **Cultura**

Ministério da **Saúde**

Ministério da **Educação**

Ministério da **Ciência, Tecnologia e Inovação**