CSIRT

As melhorias no processo de tratamento de incidentes de segurança da informação na UFRJ

Roteiro

1. A SegTIC
2. O Projeto
3. Dificuldades Enfrentadas
4. Resultados Alcançados

SegTIC – Diretoria de Segurança da Informação

Missão

“Atuar na **detecção**, **resolução** e **prevenção** de incidentes de segurança da informação na Universidade Federal do Rio de Janeiro, além de elaborar ações educativas para disseminar as boas práticas de segurança da informação. Reduzir a ocorrência de incidentes de segurança da informação através do fortalecimento de ações educativas que possibilitem o estabelecimento de um sistema de segurança da informação consistente na comunidade acadêmica da UFRJ proporcionando um ambiente cada vez mais confiável, disponível e íntegro.”

Visão

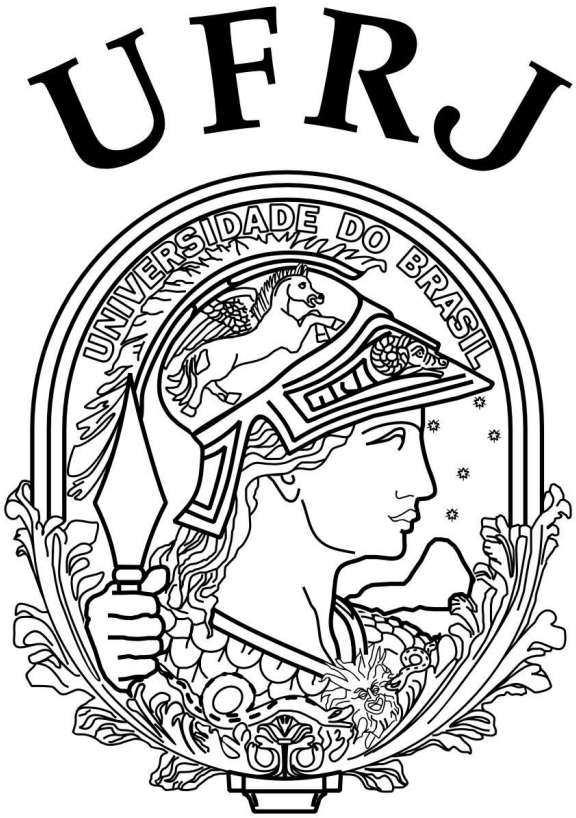
“Ser um centro de resposta e tratamento de incidentes de segurança da informação confiável, disponível e íntegro, fornecendo orientação, prevenção e informação à comunidade acadêmica da UFRJ. “

PÚBLICO ALVO (CONSTITUENCY)

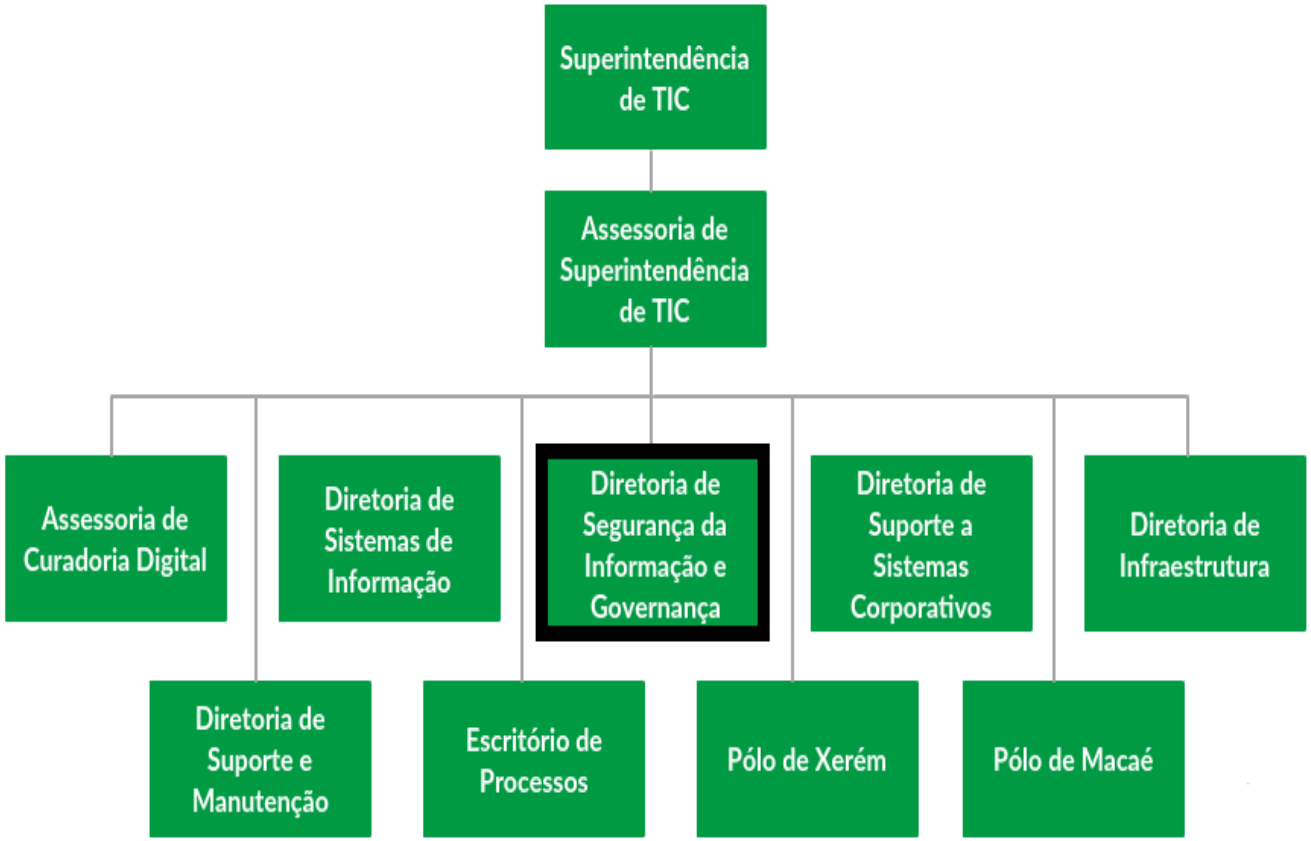
Segurança da Informação UFRJ

- Quem atendemos?

Comunidade acadêmica da UFRJ: servidores técnico administrativo, docentes, pesquisadores, alunos, bolsistas, estagiários, prestadores de serviço, pessoas que mantiverem vínculo institucional com a Universidade, bem como a sociedade que necessitar acessar os serviços on-line da Universidade.

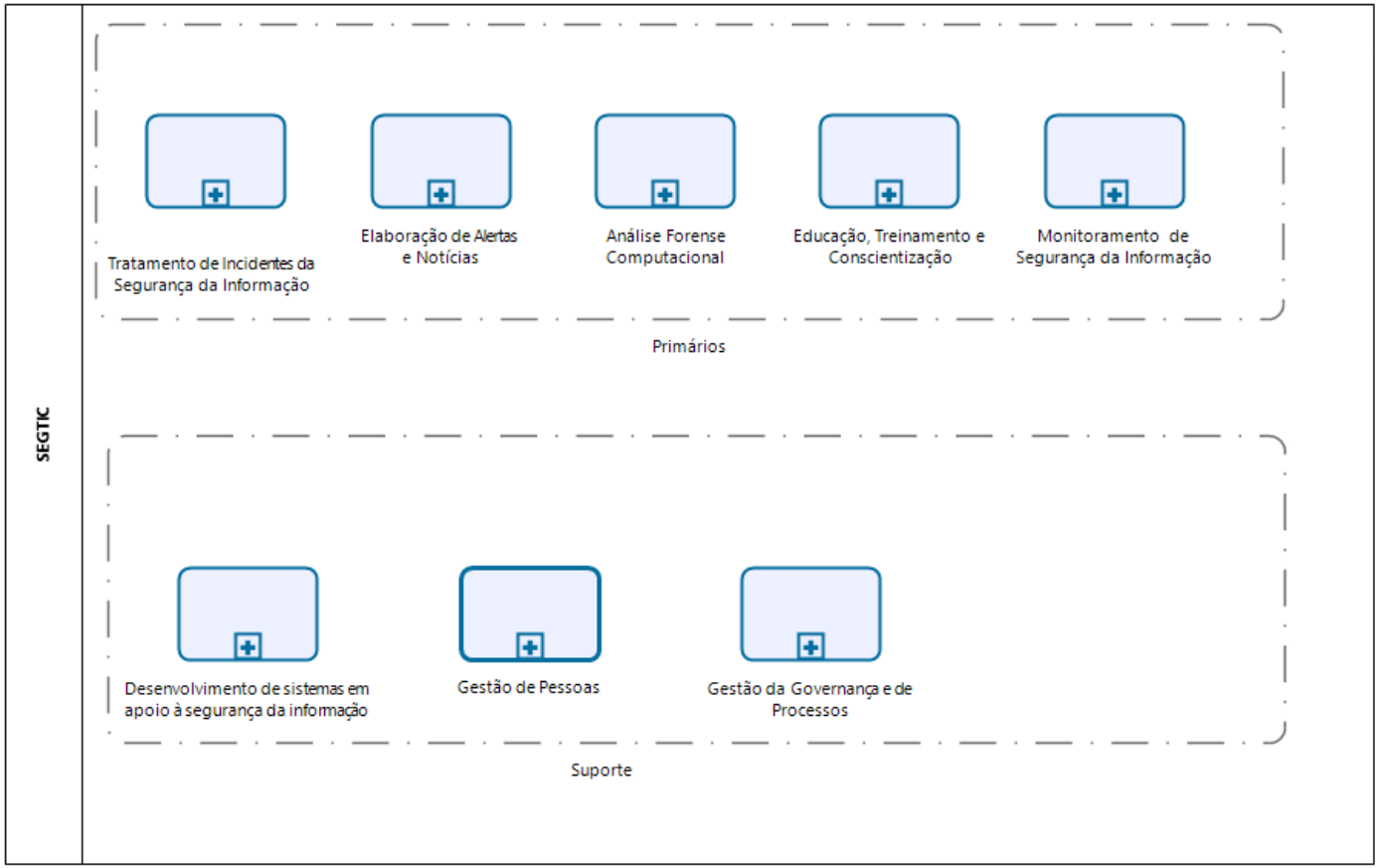


ESTRUTURA ORGANIZACIONAL



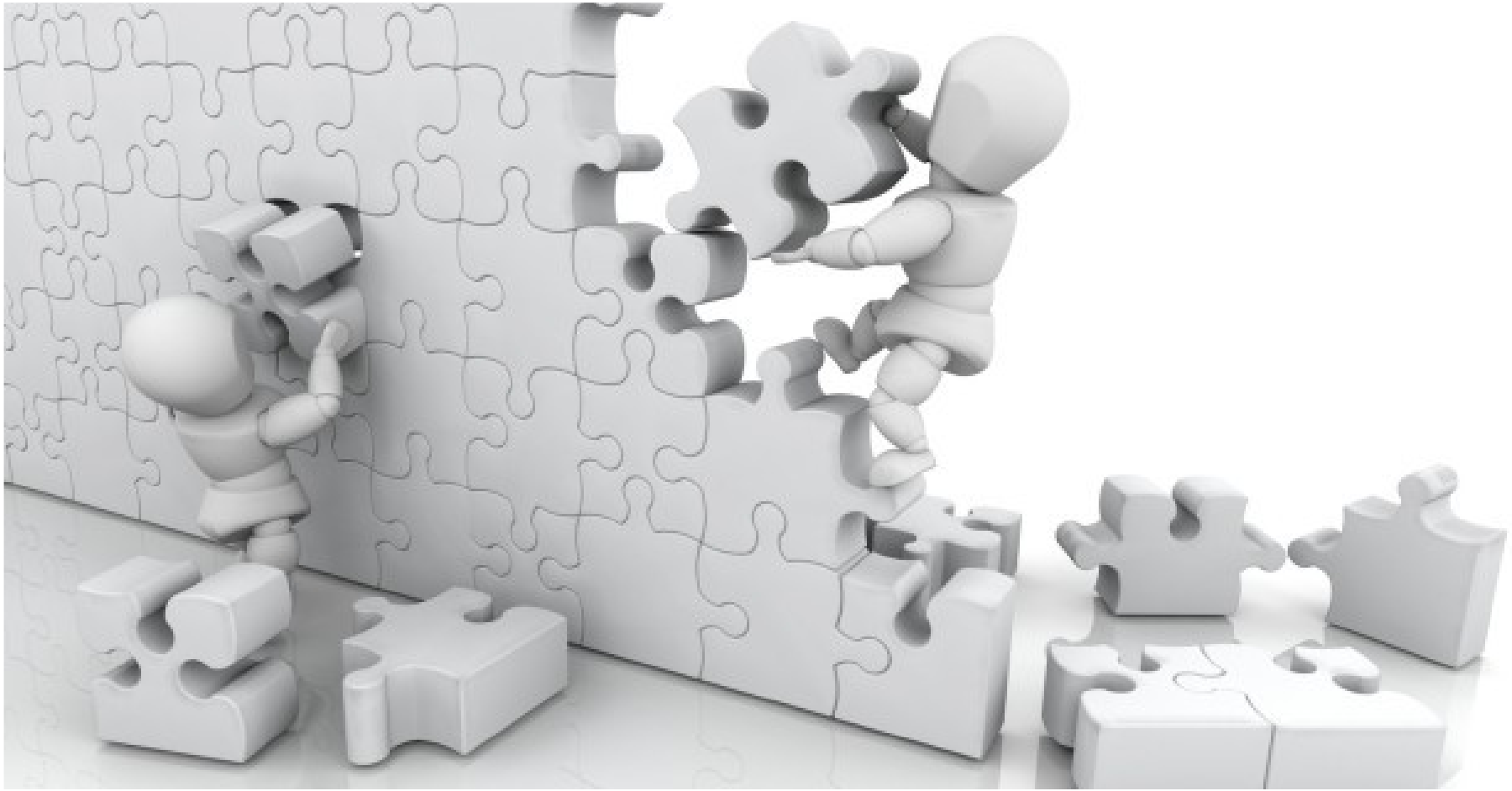
Fonte: http://tic.ufrj.br/index.php/2017-02-09-12-37-23

Macroprocessos



O Projeto

Segurança da Informação UFRJ



CSIRT – Computer Security Incident Response Team

Segurança da Informação UFRJ

Motivação

- **Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008:** Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal - APF, direta e indireta;
- **Norma Complementar nº 02/IN01/DSIC/GSIPR:** Definir a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da APF, direta e indireta;
- **Norma Complementar nº 05/IN01/DSIC/GSIPR:** Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da APF;
- **Norma Complementar nº 08/IN01/DSIC/GSIPR:** Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da APF;
- **Rede Nacional de Ensino e Pesquisa - RNP:** Programa fortalecimento da segurança da informação nas organizações usuárias.

Iniciativas

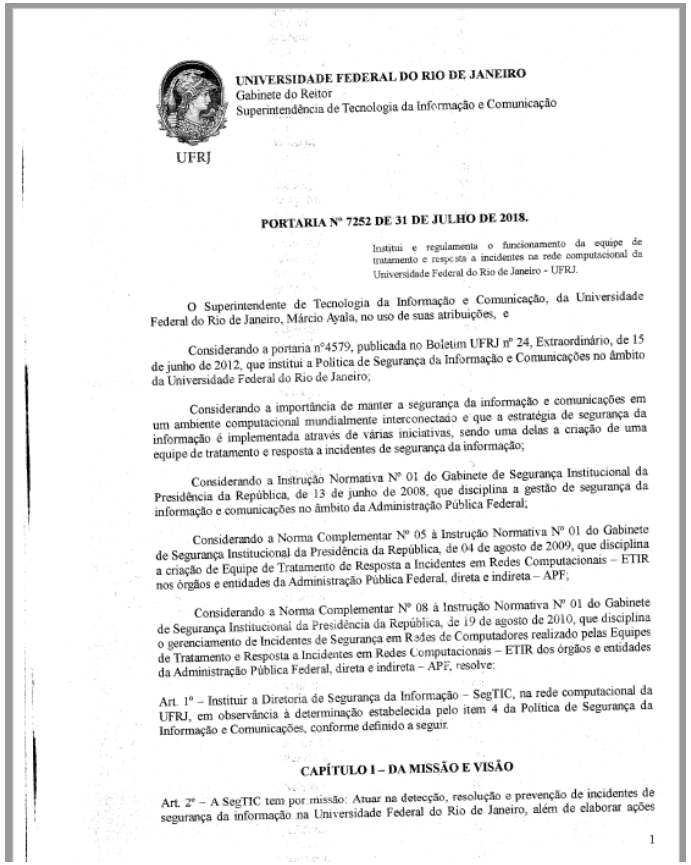
- Institucionalização do Csirt;
- Reconhecimento interno e externo;
- Melhorias na produtividade da SegTIC.

Desenvolvimento

Institucionalização do Csirt

Portaria n° 7252 de 31/07/2018:

- Institui e regulamenta o funcionamento do CSIRT da UFRJ;
- Fortalece o nosso posicionamento perante a comunidade interna e externa;
- Nos permite a adesão em grupos nacionais e internacionais para troca de experiências e apoio no tratamento de incidentes.



UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
Gabinete do Reitor
Superintendência de Tecnologia da Informação e Comunicação

UFRJ

PORTARIA Nº 7252 DE 31 DE JULHO DE 2018.

Institui e regulamenta o funcionamento da equipe de tratamento e resposta a incidentes na rede computacional da Universidade Federal do Rio de Janeiro - UFRJ.

O Superintendente de Tecnologia da Informação e Comunicação, da Universidade Federal do Rio de Janeiro, Márcio Ayala, no uso de suas atribuições, e

Considerando a portaria nº4579, publicada no Boletim UFRJ nº 24, Extraordinário, de 15 de junho de 2012, que institui a Política de Segurança da Informação e Comunicações no âmbito da Universidade Federal do Rio de Janeiro;

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 Diretoria de Segurança da Informação – SegTIC, na rede computacional da UFRJ, em observância à determinação estabelecida pelo item 4 da Política de Segurança da Informação e Comunicações, conforme definido a seguir.

CAPÍTULO I – DA MISSÃO E VISÃO

Art. 2º – A SegTIC tem por missão: Atuar na detecção, resolução e prevenção de incidentes de segurança da informação na Universidade Federal do Rio de Janeiro, além de elaborar ações

1

Desenvolvimento

- Conquistar reconhecimento interno e externo:
  - Comprometimento em comunicar as ocorrências de incidentes de segurança ao CAIS – Centro de Atendimento a Incidentes de Segurança da Informação da RNP no intuito de gerar estatísticas e soluções integradas;
  - Participação na lista de Csirt do Cert.br – Centro de Estudos, Resposta e Tratamento a Incidentes Segurança do Brasil;
  - Divulgação da SegTic nos processos de acolhimentos dos novos servidores da UFRJ;

Desenvolvimento

- Melhorias nos processos da SegTIC:
  - Identificação dos processos, primários e de suporte;
  - Identificação, priorização e mapeamento do processo crítico: **Tratamento de Incidentes de Segurança da Informação**
  - Análise da situação atual: apontar solução de problemas;
  - Indicar melhorias;
  - Elaboração e implantação de planos de ação;
  - Monitoramento dos planos de ação.

Dificuldades Enfrentadas

Dificuldades enfrentadas

- Equipe pequena x volume de trabalho;
- Capacitação da equipe;
- Reuniões de equipe para o projeto.

Resultados Alcançados

Segurança da Informação UFRJ

Melhorias

- Processos Mapeados;
- Problemas identificados;
- Melhorias apontadas;

Outros benefícios obtidos

- Visão sistêmica do setor;
- Estabelecimento de responsabilidades;
- Integração da equipe com o processo.

O que está por vir...

- Política de Segurança da Informação e Comunicação;

- Sistema de gerenciamento de incidentes;
  - Padronização das ações de tratamento de incidentes;
  - Sistema de Medição de Desempenho.

Obrigada!

Lilian da Silva Chagas

Analista de Tecnologia da Informação
Diretoria de Segurança da Informação - SegTIC/UFRJ
lilianchagas@tic.ufrj.br