WORKSHOP CTIC 2019

CSIC

Coordenadoria de Segurança da Informação e Comunicação

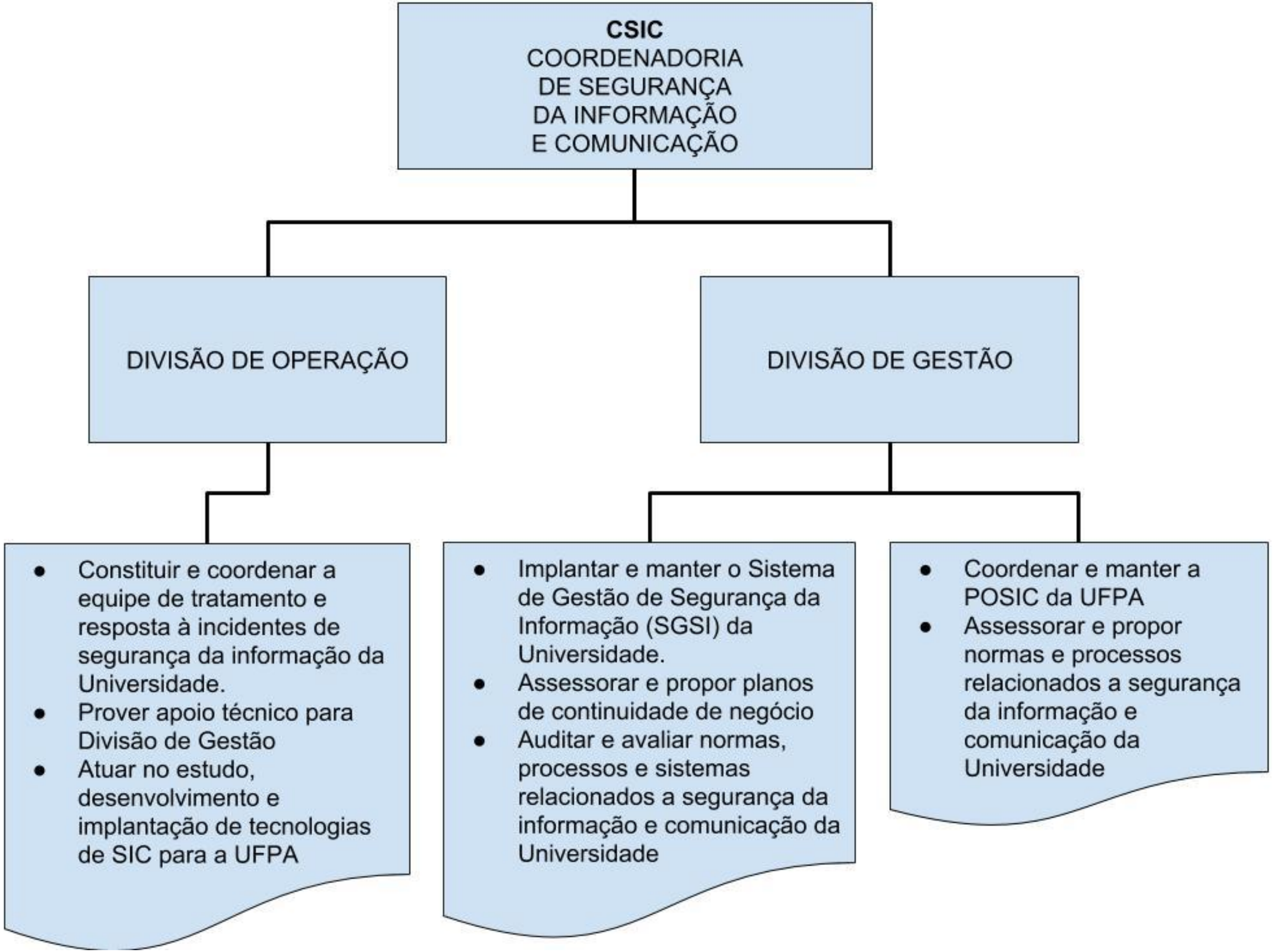
MISSÃO

- Auxiliar a UFPA para manter a segurança de TIC
- Auxiliar a UFPA com soluções de segurança de TIC
- Auxiliar a UFPA na criação e manutenção de normas relacionadas a segurança de TIC

EQUIPE

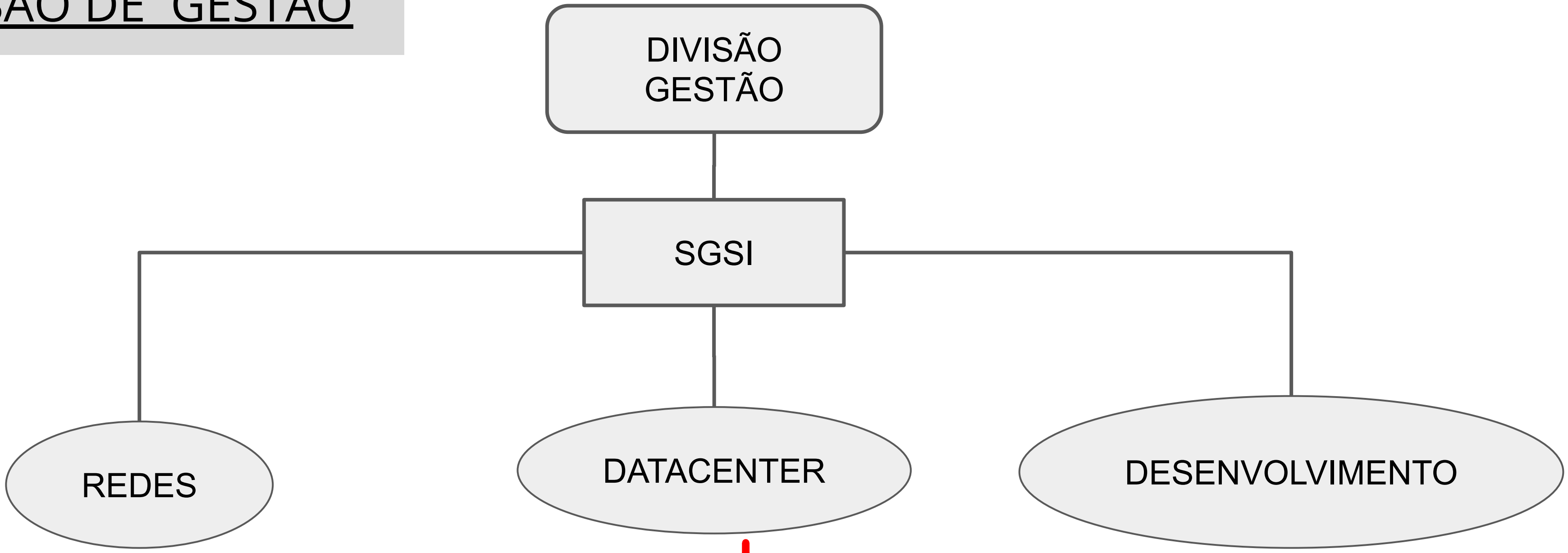
- Rômulo Pinto de Albuquerque - Coordenador CSIC
- Jéssica Janile Monteiro de Castilho - Chefe Div. Gestão
- Jean Carlos Felix de Freitas - Chefe Div. Operação
- Bolsistas:
    - José Ferreira, Kaio Cesar, Elayla Brito, Jordhan Henrique, Gustavo Damasceno, Kaíque da Silva, Daniel Morais

ESTRUTURA


CSIC
COORDENADORIA
DE SEGURANÇA
DA INFORMAÇÃO
E COMUNICAÇÃO
DIVISÃO DE OPERAÇÃO
DIVISÃO DE GESTÃO
● Constituir e coordenar a equipe de tratamento e resposta à incidentes de segurança da informação da Universidade.
● Prover apoio técnico para Divisão de Gestão
● Atuar no estudo, desenvolvimento e implantação de tecnologias de SIC para a UFPA
● Implantar e manter o Sistema de Gestão de Segurança da Informação (SGSI) da Universidade.
● Assessorar e propor planos de continuidade de negócio
● Auditar e avaliar normas, processos e sistemas relacionados a segurança da informação e comunicação da Universidade
● Coordenar e manter a POSIC da UFPA
● Assessorar e propor normas e processos relacionados a segurança da informação e comunicação da Universidade

ATIVIDADES

DIVISÃO DE GESTÃO



- ISO 27001
- ISO 27002

Realizar a gestão de um processo crítico

- Gestão e classificação de ativos
- Mapa de vulnerabilidades
- Controles

ATIVIDADES

DIVISÃO DE GESTÃO - Jéssica Janile

Em 2019:

- Atuação no atendimento de demandas da DIV. OPERAÇÃO:
  - Migração do antigo firewall (bacuri) para o firewall fortigate 300D
  - Anti-spam
  - Criação/manutenção de regras no firewall
  - Criação/manutenção de VPNs para rede DMZ
  - Análise de logs no Forti Analizer

ATIVIDADES

DIVISÃO DE GESTÃO - Jéssica Janile

Em 2019:

- Atuação no atendimento de demandas da DIV. DE OPERAÇÃO:
  - Prevenção, tratamento e resposta à incidentes - CSIRT
  - Manutenção do site do CSIRT
- Específico da DIV. DE GESTÃO **(2019-2020)**
  - Estudo Lei Geral de Proteção de Dados - **LGPD**
  - Criação da norma de **controle de acesso do CTIC**
  - Pesquisa sobre solução de **gestão de ativos**

ATIVIDADES

DIVISÃO DE OPERAÇÃO - Jean Freitas

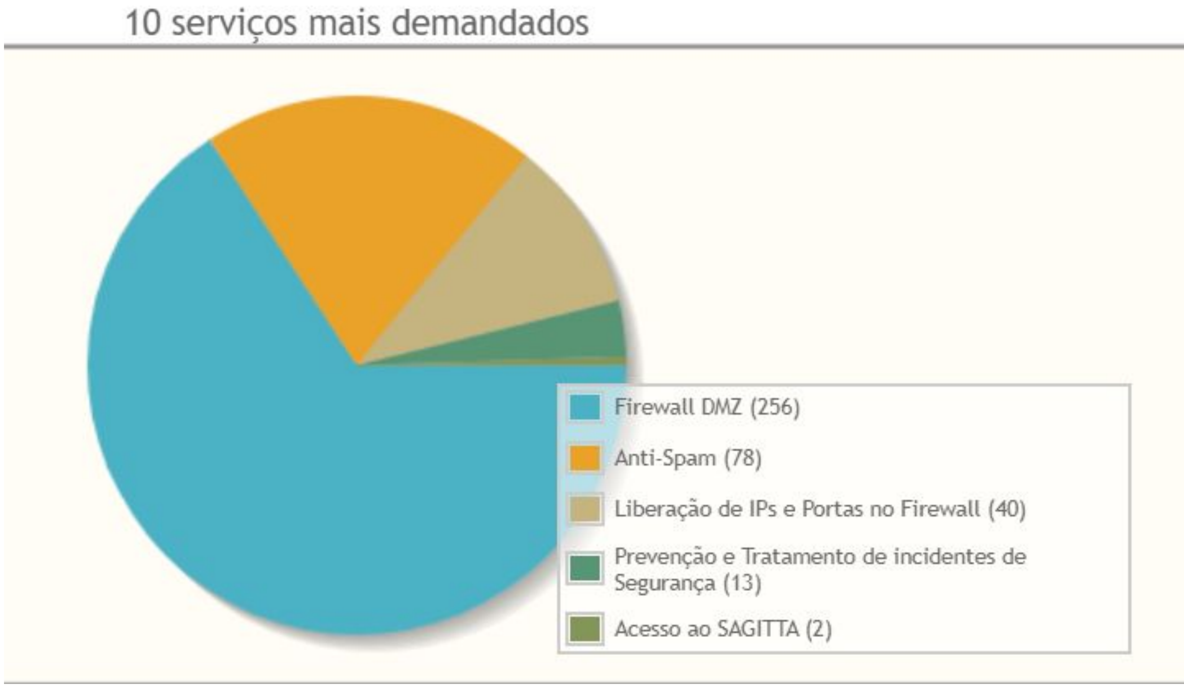
Em 2019:

- Migração do antigo firewall (bacuri) para o firewall fortigate 300D
- Anti-spam
- Criação/manutenção de regras no firewall
- Criação/manutenção de VPNs para rede DMZ
- Análise de logs no Forti Analizer
- Prevenção, tratamento e resposta à incidentes - CSIRT
- Gestão e operação do Request Tracker - RT
- Gestão e operação do Anti-spam

ATIVIDADES

SAGITTA

- **Chamados abertos: 349**
- **Chamados fechados: 348**
- **Chamados em atendimento: 1**



CSIRT

- **Norma Complementar Nº 5 de 2009** - DSIC (Departamento de Segurança Info. Comun.)
- Site: https://csirt.ufpa.br
- **CSIRT UFPA** Surgiu com a parceria da RNP a partir de 2017
- Estabelecimento em Julho de 2018
- Canais de contato
    - E-mail csirt@ufpa.br
    - Sagitta

CSIRT

- **Membros:**
  - **Rômulo Albuquerque (Coordenador) - CSIC**
  - **Jean Freitas - CSIC**
  - **Jéssica Monteiro - CSIC**
  - **Gabriel Silva - Datacenter**
  - **João Salvatti - Redes**
  - **Rafael Feitosa - Sistemas**
  - **Jnane Neiva - Atendimento**

CSIRT

SITE

Ir para o conteúdo 1
Ir para o menu 2
Ir para a busca 3
Ir para o rodapé 4
ACESSIBILIDADE
ALTO CONTRASTE
MAPA DO SITE
Universidade Federal do Pará
CSIRT UFPA
CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
Buscar no portal
Perguntas frequentes
Contato
SOBRE O CSIRT
Apresentação
Organizacional
Serviços
Equipe
Contato
DOCUMENTOS
Política de Segurança da Informação e Comunicação
Instrução Normativa - Email Institucional
Instrução Normativa -
Ações em Destaque
CSIRT
Saiba mais como funciona o CSIRT da UFPA

CSIRT - RT (Sistema de Chamados)

Início Buscar Artigos Ferramentas Admin TRAIRA Entrou como root

RT para rt.csirt.ufpa.br BEST PRACTICAL

Encontrados 4 tíquetes

Novo tíquete em | Abuso Acess

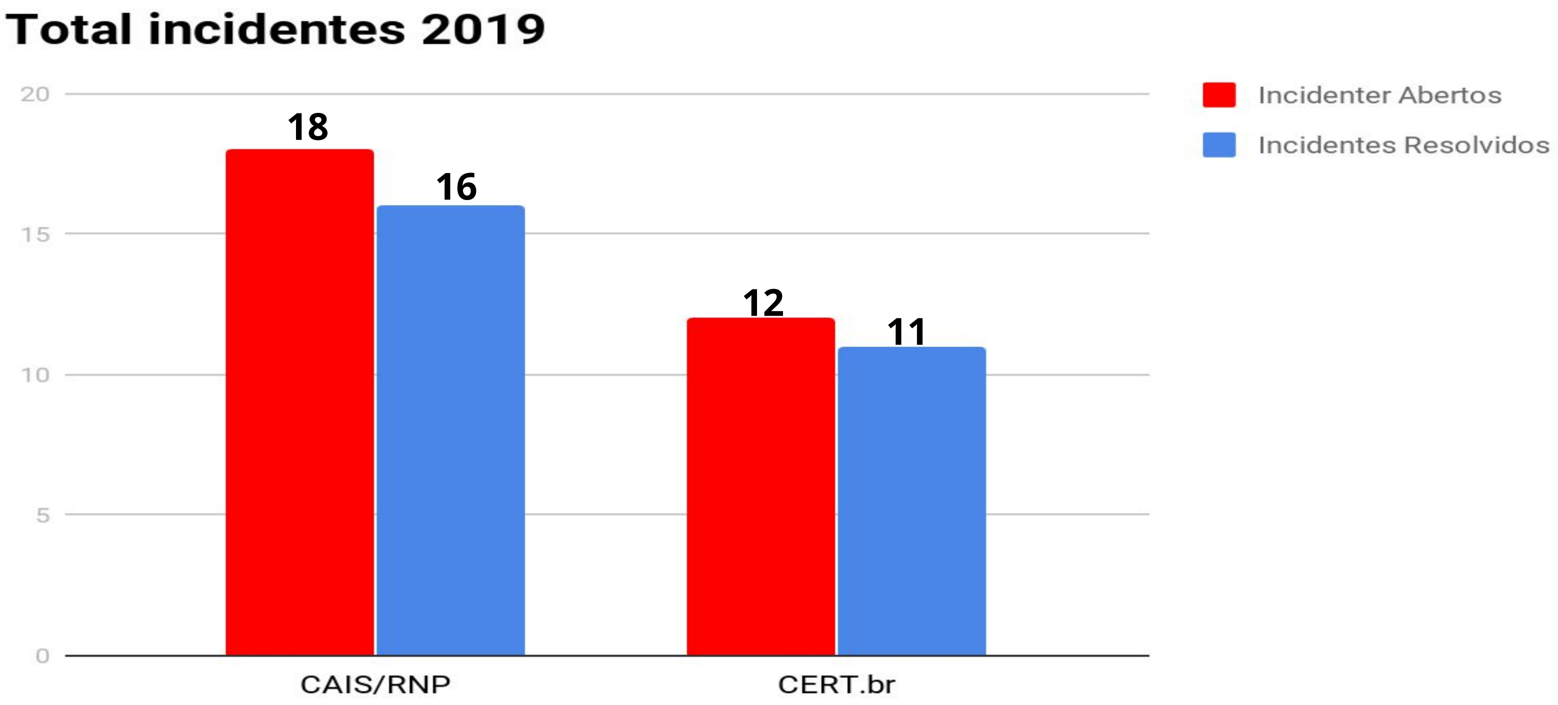
Editar Busca | Avançado | Apresentar Resultados | Atualização em Massa | Gráfico | Fontes de Notícias

#	Assunto / Requisitante	Estado / Criado	Fila / Última atualização	Proprietário / Atualizado em	Prioridade / Tempo Restante
1000111	**[CAIS #4096569] Host(s) infectado(s) com malware [aberto]** <cais@cais.rnp.br>	aberto 3 semanas atrás	BotNet	janile (Jessica Janile Monteiro de Castilho) 3 semanas atrás	50
1000116	Bloqueio de computador Walkyria Magno <walkyriamagno@gmail.com>	novo 5 dias atrás	General	Nobody in particular 5 dias atrás	50
1000119	**[CAIS #4117376] Desfiguração de Site [aberto]** <cais@cais.rnp.br>	novo 16 horas atrás	Defacement	gabrielp (Gabriel Silva Pinto) 5 horas atrás	50
1000120	**Desfiguracao de website (iedaguedes.ufpa.br)** <cert@cert.br>	novo 6 horas atrás	Defacement	gabrielp (Gabriel Silva Pinto) 5 horas atrás	50

Não recarregar esta página. | Alterar

BEST PRACTICAL

CSIRT


Total incidentes 2019
20
15
10
5
0
18
16
12
11
CAIS/RNP
CERT.br
Incidenter Abertos
Incidentes Resolvidos

CSIRT

Principais Tipos de Incidentes:

- DDoS
- Bot Net
- Desfiguração de site
- Vazamento de dados

PLANOS PARA 2020

- Auxílio na implantação da LGPD
- Monitoramento de eventos de segurança em computadores
- Análise de vulnerabilidades servidores SIG
- Atualização infraestrutura de servidores
- Palestras e cursos