

---

---

# WORKSHOP CTIC 2023

**CSIC**

Coordenadoria de Segurança da  
Informação e Comunicação

---

---

# ORGANIZAÇÃO DA APRESENTAÇÃO

- ➔ Apresentação da CSIC
- ➔ Atividades ano 2023
- ➔ Dificuldades/Necessidades

# MISSÃO

- Atuar em segurança de TIC no âmbito da UFPA

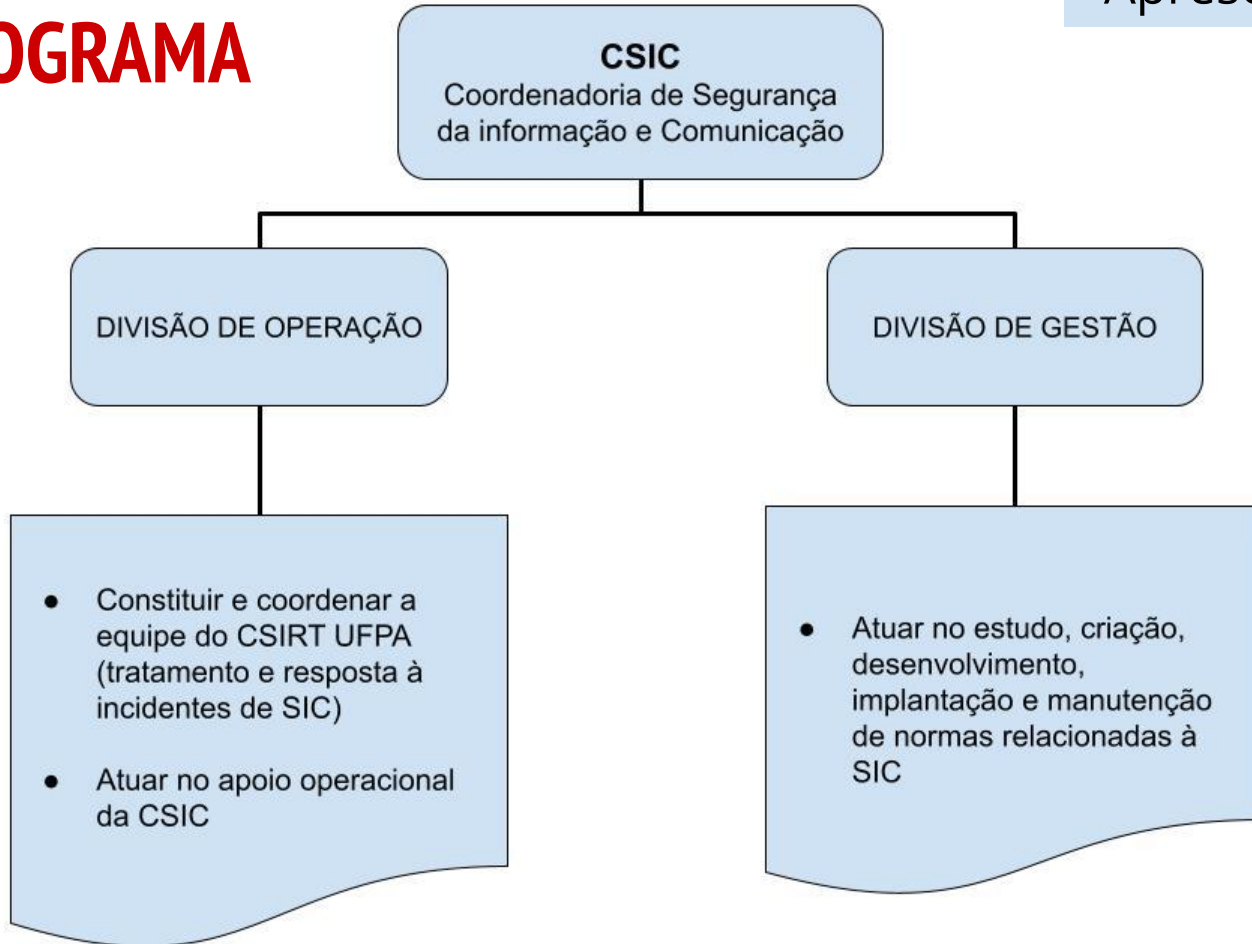
Tanto na área **operacional** com estudo, desenvolvimento, implantação e manutenção de soluções de segurança da informação e comunicação

Quanto na área de **gestão** com o estudo, criação e manutenção de normas relacionadas à segurança da informação e comunicação

# EQUIPE

- Rômulo Pinto de Albuquerque - **Coordenador CSIC**
- Jéssica Janile Monteiro de Castilho - **Chefe Div. Gestão**
- Jean Carlos Felix de Freitas - **Chefe Div. Operação**
- Bolsistas:
  - Danilo Ren Nicioka
  - Elienai da Costa Soares

# ORGANOGRAMA



# NORMATIVOS

- Política de segurança da informação e comunicação (POSIC)
- Política de gestão de ativos de TIC
- Política de backup e recuperação de dados
- Plano de gestão de riscos de TI
- Plano de continuidade de negócios de TI
- Plano de gestão de incidentes
- Instrução normativa de utilização e acesso aos recursos de TIC

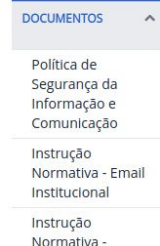
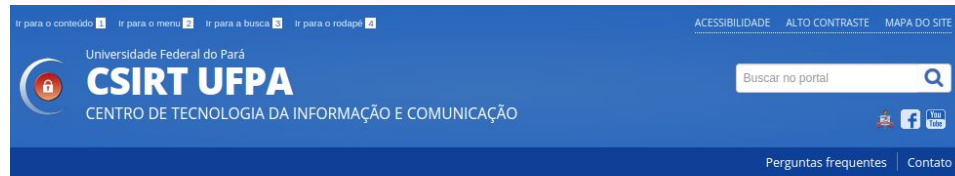


<https://governancadigital.ufpa.br/>

# CSIRT UFPA

- **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](mailto:csirt@ufpa.br)
  - Sagitta

<https://csirt.ufpa.br>



### Ações em Destaque



Saiba mais como funciona o CSIRT da UFPA

# CSIRT UFPA

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

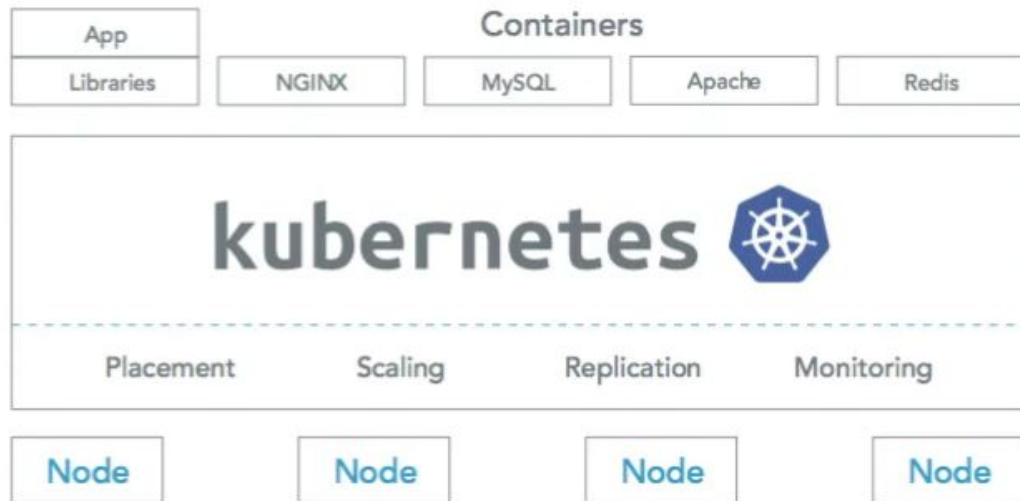
Portaria: [link](#)



# INFRAESTRUTURA

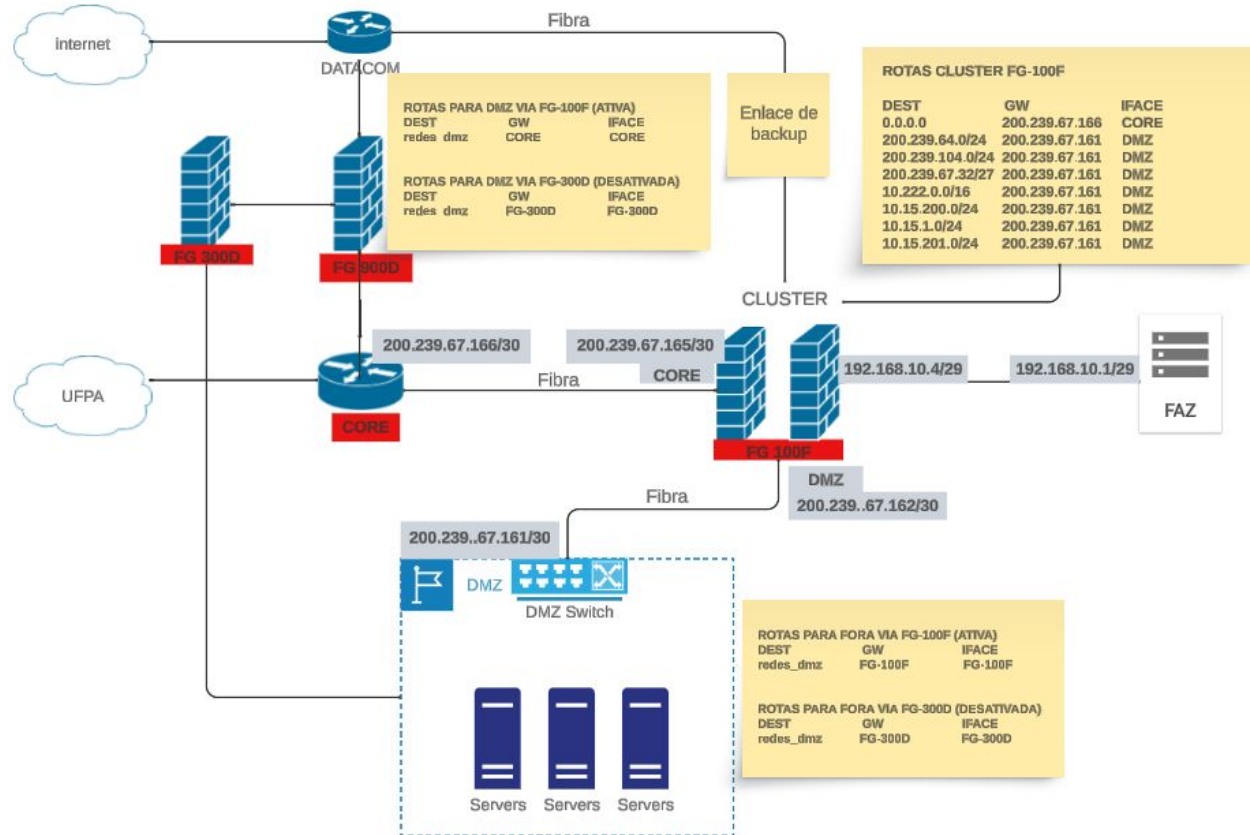
## SERVIDOR DELL POWEREDGE R730

- CPU: 40
- RAM: 128G



# INFRAESTRUTURA

**FORTIGATE 300D -> 100F**  
- Firewall DMZ



# INFRAESTRUTURA

## Anti Spam McAfee

- Fim de linha desde 2021
- Não tem mais suporte
- **Não recomende seu uso!!!**



# WAZUH - Gestão de vulnerabilidades

Atividades ano 2023



12 servidores  
ativos



Total de vulnerabilidades identificadas no início do funcionamento da ferramenta



Figura 1. Total de vulnerabilidades

Total de vulnerabilidades corrigidas até o período atual



Figura 2. Vulnerabilidades solucionadas

# OCS Inventory - Gestão de ativos

Atividades ano 2023



## My dashboard

<b>49</b> Machine(s)	<b>36</b> Windows	<b>13</b> Unix	<b>0</b> Android	<b>0</b> Others	<b>11</b> Operating system	<b>19614</b> Software
-------------------------	----------------------	-------------------	---------------------	--------------------	-------------------------------	--------------------------

## Machines contacted today

<b>30</b> Total	<b>19</b> Windows	<b>11</b> Unix	<b>0</b> Android
--------------------	----------------------	-------------------	---------------------

<https://servicosdetic.ufpa.br/>

# Bem vindos!

A divisão de segurança da internet do CTIC mantém um grupo de ação de resposta rápida - o "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança. É uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança computadores. O CSIRT UFPA presta serviços para uma comunidade acadêmica, relatando invasões e resolve problemas relacionados à segurança computacional. Para acessar informações detalhadas sobre segurança internet, acesse [CSIRT - UFPA](#).

## Tutoriais

- [Antivirus](#)
- [Autenticação em duas etapas: Google Authenticator](#)
- [Autenticação em duas etapas: LastPass Authenticator](#)
- [Backup do e-mail Institucional - G Suite UFPA](#)
- [Criptografia utilizando o Veracrypt](#)
- [Criptografia PGP no e-mail](#)
- [Configurações de segurança do Google Workspace](#)
- [Configurações de segurança no Windows 10](#)
- [Configurações de atualização de segurança no Windows 10](#)

Instrução Normativa de utilização e acesso aos recursos de TIC

[Instrução normativa sobre utilização de sua conta institucional nos serviços de TIC da UFPA](#)

### Correio Eletrônico

- Abertura, Recuperação e Fechamento de E-mail
- Anti-Spam
- Gestão de Conta de E-mail
- Google Workspace (G Suite)
- Grupo de E-mail

### Serviços On-Line

- Conta Institucional
- Microsoft 365
- Prevenção e Tratamento de incidentes de Segurança

### Suporte Computacional

- Compartilhamento de arquivos
- Diagnóstico / Avaliação / Instalação PC
- Impressoras/Scanner
- Instalação ou remoção de programas
- Manutenção de Computadores

### Hospedagem de Sites e Serviços

- Adição ou Remoção de Usuário Externo
- Sites Institucionais e seus Assuntos

### Serviços de Redes

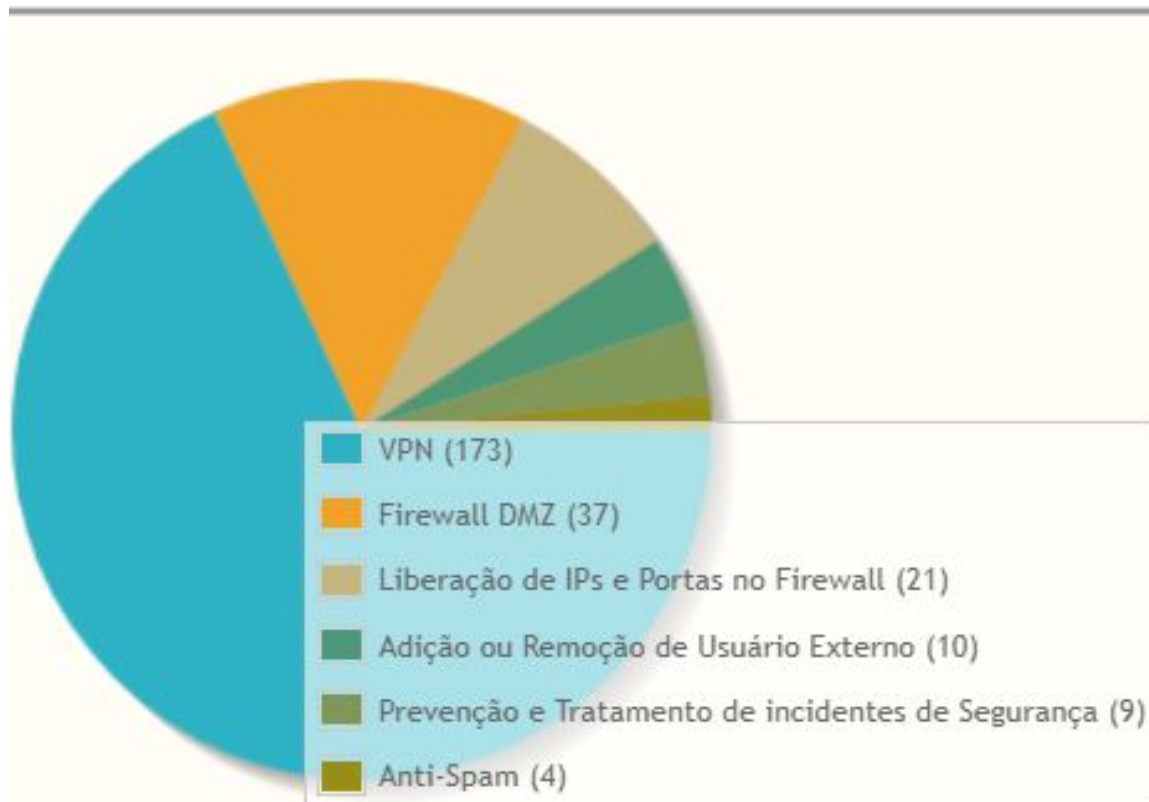
- Endereçamento IP e DHCP Institucional
- Liberação de IPs e Portas no Firewall
- Limitação de Acesso a Sites e Serviços de Internet
- Serviços Internos
- VPN

### Demanda Interna

- Demanda Coord. de Atendimento
- Demanda Interna Data Center
- Firewall DMZ

## 10 serviços mais demandados

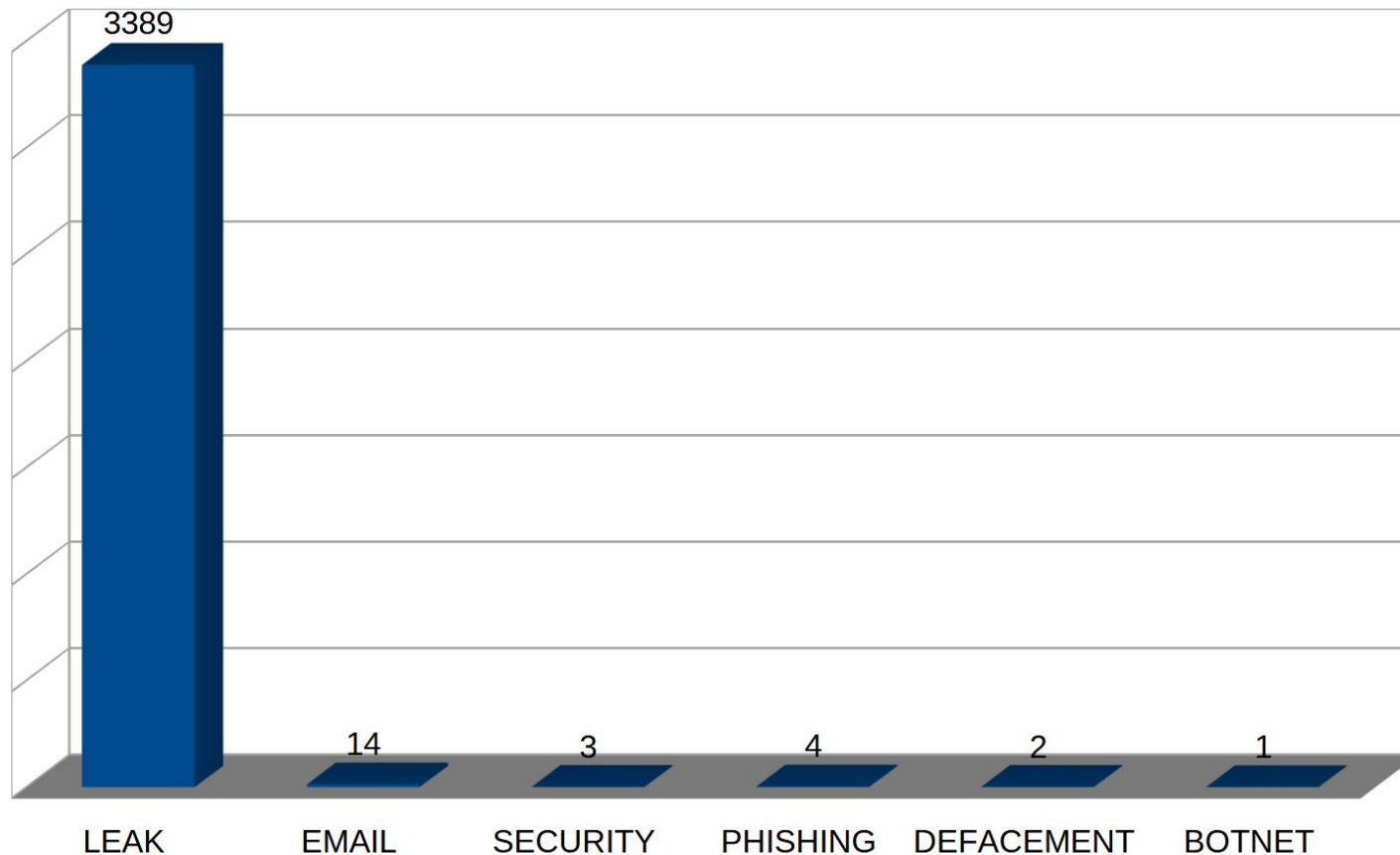
Total de chamados abertos no ano de 2023: **254**





# CSIRT - Request Tracker

Atividades ano 2023



# AXUR - Vazamento de dados

Atividades ano 2023



Adicionar filtro    Buscar ticket

Detectado nos últimos 12 meses ×

Abertos 0

**Incidentes 5.470**

Tratamento 0

Encerrados 1

# PoC - Prova de Conceito

Atividades ano 2023



Gestão de vulnerabilidades



Vazamento de dados

❖ Consulta de vazamentos

❖ Notificação

Parado

WAF



Web Application Firewall  
Proteção de aplicações web

Em andamento ...

# MIGRAÇÃO FIREWALL

Atividades ano 2023

- FIREWALL ATUAL -> FORTIGATE 300D (Fim de suporte)
- AQUISIÇÃO FIREWALL **FORTINET 100F**
  - Atuação conjunta: **CSIC + DATACENTER + REDES**



Add cover Add comment

## Migração firewall fortigate FG 100F

List view

### Atividades

● Not started 1

Migração das regras do FG 300D

+ New

+ New

● In progress 0

● Done 4

Configuração básica

Desenho da rede

Configuração com FortiAnalyzer

Ativação licença

# CURSOS E PALESTRAS

- CAPACIT
  - Boas práticas de segurança da informação na UFPA
  - Abril de 2023
- Webinar LGPD - Tutorial de tarjamento

# DIFICULDADES/NECESSIDADES

- ❖ **Perda de 6 bolsistas nos últimos anos**
  - Começou em 2017 com **8**, agora são **2**
- ❖ **Formação de uma equipe de SOC (Fazemos apenas o básico)**
  - monitoramento
  - tratamento e resposta à incidentes
  - gestão de vulnerabilidades
  - pentest