
WORKSHOP CTIC 2024

CSIC

Coordenadoria de Segurança da
Informação e Comunicação

ORGANIZAÇÃO DA APRESENTAÇÃO

- ➔ Apresentação da CSIC
 - ➔ Atividades ano 2024
 - ➔ Status PDU 2022-2025
 - ➔ 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

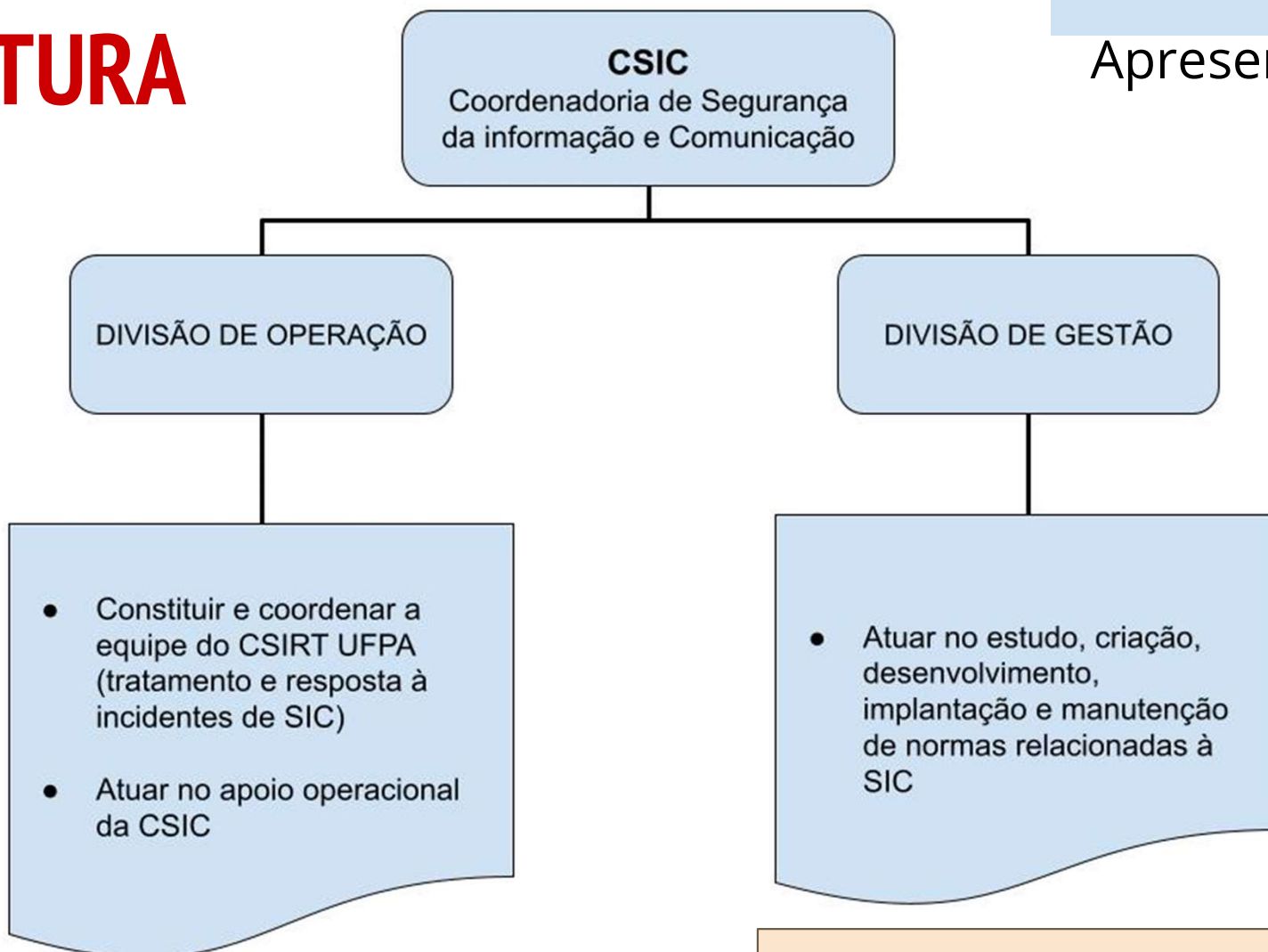
EQUIPE

Apresentação da CSIC

- Jéssica Janile Monteiro de Castilho
- Jean Carlos Felix de Freitas
- Bolsistas:
 - Danilo Ren Nicioka
 - Jean Dean

ESTRUTURA

Apresentação da CSIC



<https://csirt.ufpa.br>

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

CSIRT UFPA

Apresentação da CSIC

- **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

<https://csirt.ufpa.br>



Ações em Destaque



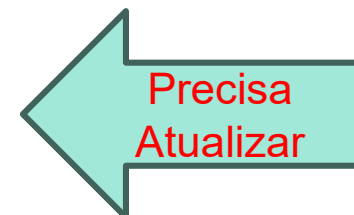
Saiba mais como funciona o CSIRT da UFPA

CSIRT UFPA

Apresentação da CSIC

- **Membros:**

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



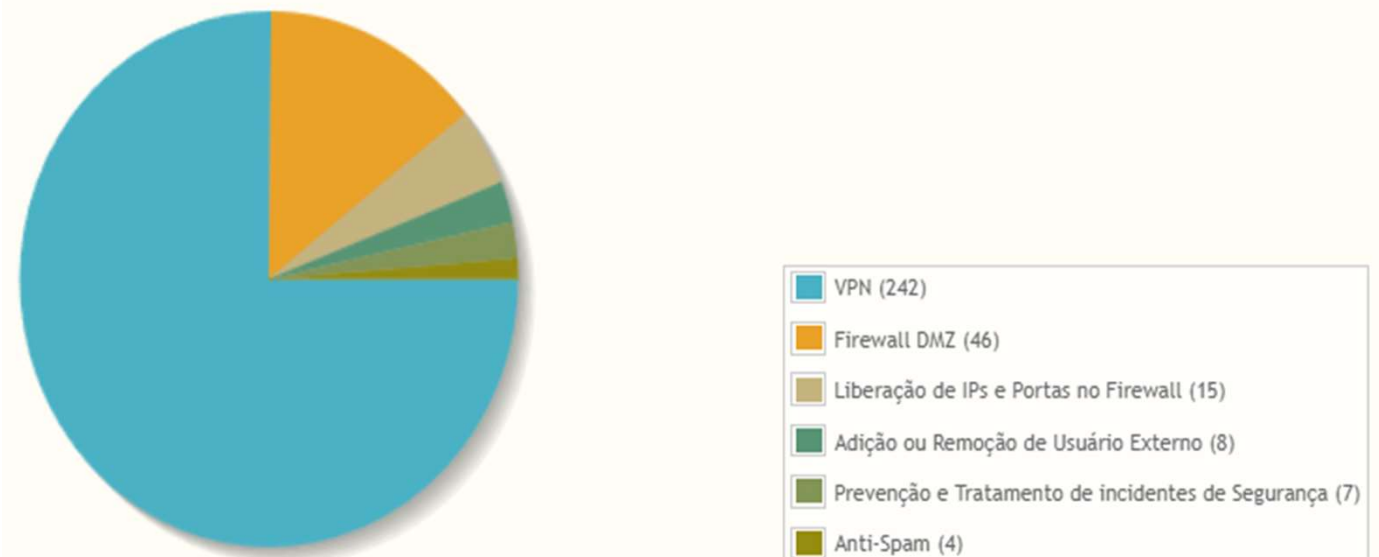
Portaria: [link](#)

SAGITTA

Atividades ano 2024

- Chamados abertos: 322
- Chamados atendidos: 310

10 serviços mais demandados



INFRAESTRUTURA

Atividades ano 2024

Conclusão Migração

FORTIGATE 300D -> 100F

- Firewall DMZ








INFRAESTRUTURA

Atividades ano 2024

- Segmentação da rede do SIG → evitar movimentação lateral

Interface	 SIG-BD_DESENVOLVIMENTO (SIG-DB_DEV)
Alias	SIG-BD_DESENVOLVIMENTO
Link	 1 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	 VLAN
Role	LAN
	
Base Interface	 DMZ (dmz)

Interface	 DMZ (dmz)
Alias	DMZ
Link	 1 Gbps Full Duplex
Port Speed	Auto-Negotiation
Type	 Physical Interface
Role	DMZ
	
HA Role	 HA Monitor Interface

2024

PDU 2022-2025

Unidade: CTIC

Subunidade responsável: CSIRT

Iniciativa Tática: Ampliar e consolidar a Segurança cibernética e a Segurança da Informação

Objetivo da iniciativa: Assegurar a disponibilidade de sistemas essenciais de Tecnologia da Informação

Responsável pela iniciativa: Rômulo Albuquerque / Jéssica Janile

Nº	Processos/Ações	Custo	Responsável	Prazo			Status Observações
				Início	Previsão de Fim	Fim	
01	Aquisição, instalação e configuração de equipamentos de TI (firewalls e analisador de logs) para a segurança da informação	R\$ 1.450.000,00	Rômulo Albuquerque e Jéssica Janile	06/2023	12/2023		Não iniciado
02	Implantar um serviço de TI para o inventário de hardware e software para toda a comunidade da UFPA	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	06/2022	12/2022		Em andamento
03	Implantar um sistema de verificação de vazamento de dados dos usuários de e-mail da UFPA	R\$ 40.000,00	Rômulo Albuquerque e Jéssica Janile	01/2023	12/2023		Não iniciado
04	Diagnosticar vulnerabilidades nos serviços de TIC institucionais	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	03/2023	07/2024		Não iniciado
05	Aplicar correções de vulnerabilidades em serviços de TIC institucionais	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	08/2023	12/2024		Não iniciado
06	Implantar o registro de logs de ativos e serviços de TIC	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	03/2023	03/2024		Não iniciado
07	Aquisição, instalação e configuração de solução de software para segurança da informação aplicada à LGPD	R\$ 430.000,00	Rômulo Albuquerque e Jéssica Janile	06/2023	12/2023		Não iniciado
08	Implantar cursos de capacitação sobre segurança da informação na UFPA	R\$ 0,00	Rômulo Albuquerque	06/2022	12/2022		Em andamento

Status: Em andamento normal; com atrasos não críticos; em atraso; concluído e não iniciado.

2024

PDU 2022-2025

Nº	Processos/Ações	Custo	Responsável	Prazo			Status Observações
				Início	Previsão de Fim	Fim	
01	Aquisição, instalação e configuração de equipamentos de TI (firewalls e analisador de logs) para a segurança da informação	R\$ 1.450.000,00	Rômulo Albuquerque e Jéssica Janile	06/2023	12/2023		Não iniciado



FORTINET®



Managed FortiAnalyzer

500 MB tägliches Logvolumen by ENBITCON

www.enbitcon.de

2024

PDU 2022-2025

02	Implantar um serviço de TI para o inventário de hardware e software para toda a comunidade da UFPA	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	06/2022	12/2022		Em andamento
----	--	----------	-------------------------------------	---------	---------	--	--------------



reportar

My dashboard



13 Máquinas	8 Windows	5 Unix	0 Android	0 Others	8 Sistema Operacional	9312 Software
-----------------------	---------------------	------------------	---------------------	--------------------	---------------------------------	-------------------------

Máquinas que se reportaram hoje

8 Total	3 Windows	5 Unix	0 Android
-------------------	---------------------	------------------	---------------------

2024

PDU 2022-2025

03	Implantar um sistema de verificação de vazamento de dados dos usuários de e-mail da UFPA	R\$ 40.000,00	Rômulo Albuquerque e Jéssica Janile	01/2023	12/2023	Não iniciado
----	--	---------------	-------------------------------------	---------	---------	--------------

AXUR
INFORMATION SECURITY



Vazamento de dados

- ❖ Consulta de vazamentos
- ❖ Notificação



(CISC Gov.br) fornecer as mesmas informações

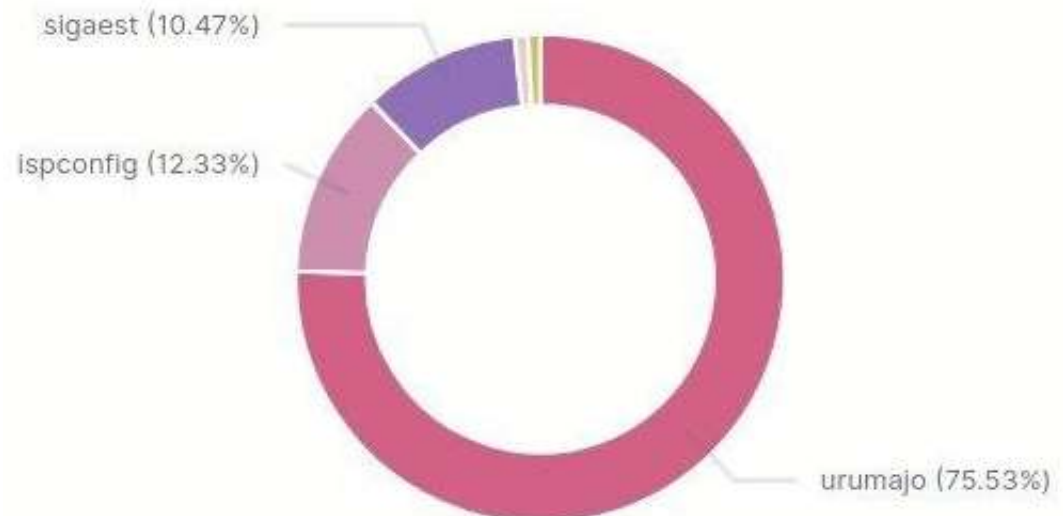
2024

PDU 2022-2025

04	Diagnosticar vulnerabilidades nos serviços de TIC institucionais	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	03/2023	07/2024	Não iniciado
05	Aplicar correções de vulnerabilidades em serviços de TIC institucionais	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	08/2023	12/2024	Não iniciado

CONTÍNUO

GESTÃO DE VULNERABILIDADE



O gráfico exibe os agentes que possuem mais ocorrências de alertas, registrados durante 3h ontem (02/12), onde o agente urumajo (200.239.64.162) foi o que registrou mais alertas.

2024

PDU 2022-2025

06	Implantar o registro de logs de ativos e serviços de TIC	R\$ 0,00	Rômulo Albuquerque e Jéssica Janile	03/2023	03/2024	Não iniciado
07	Aquisição, instalação e configuração de solução de software para segurança da informação aplicada à LGPD	R\$ 430.000,00	Rômulo Albuquerque e Jéssica Janile	06/2023	12/2023	Não iniciado



- Atualmente somente é utilizado o FAZ.
- Em relação a LGPD, não se tem diretivas do comitê.

2024

PDU 2022-2025

08	Implantar cursos de capacitação sobre segurança da informação na UFPA	R\$ 0,00	Rômulo Albuquerque	06/2022	12/2022		Em andamento
----	---	----------	--------------------	---------	---------	--	--------------



- CAPACIT
 - Boas práticas de segurança da informação na UFPA

PESSOAL

Necessidades

- ❖ **Perda de pessoal: 6 bolsistas e 1 servidor nos últimos anos**
 - Começou em 2017 com **8**, agora são **2**
 - Éramos em **3** servidores, agora são **2**.
- ❖ **Qualificação e treinamento da equipe**
 - Necessidade de qualificação especializada para atender as demandas da coordenadoria.
- ❖ **Formação de uma equipe de SOC**
 - monitoramento
 - tratamento e resposta à incidentes
 - gestão de vulnerabilidades
 - pentest

**MUITO
OBRIGADO!**