WORKSHOP CTIC 2022/23

CSIC

Coordenadoria de Segurança da Informação e Comunicação

ORGANIZAÇÃO DA APRESENTAÇÃO

- Apresentação da CSIC
- Atividades ano 2022
- Status PDTIC 2021-2023
- Necessidades

MISSÃO

- Atuar em segurança de TIC no âmbito da UFPA

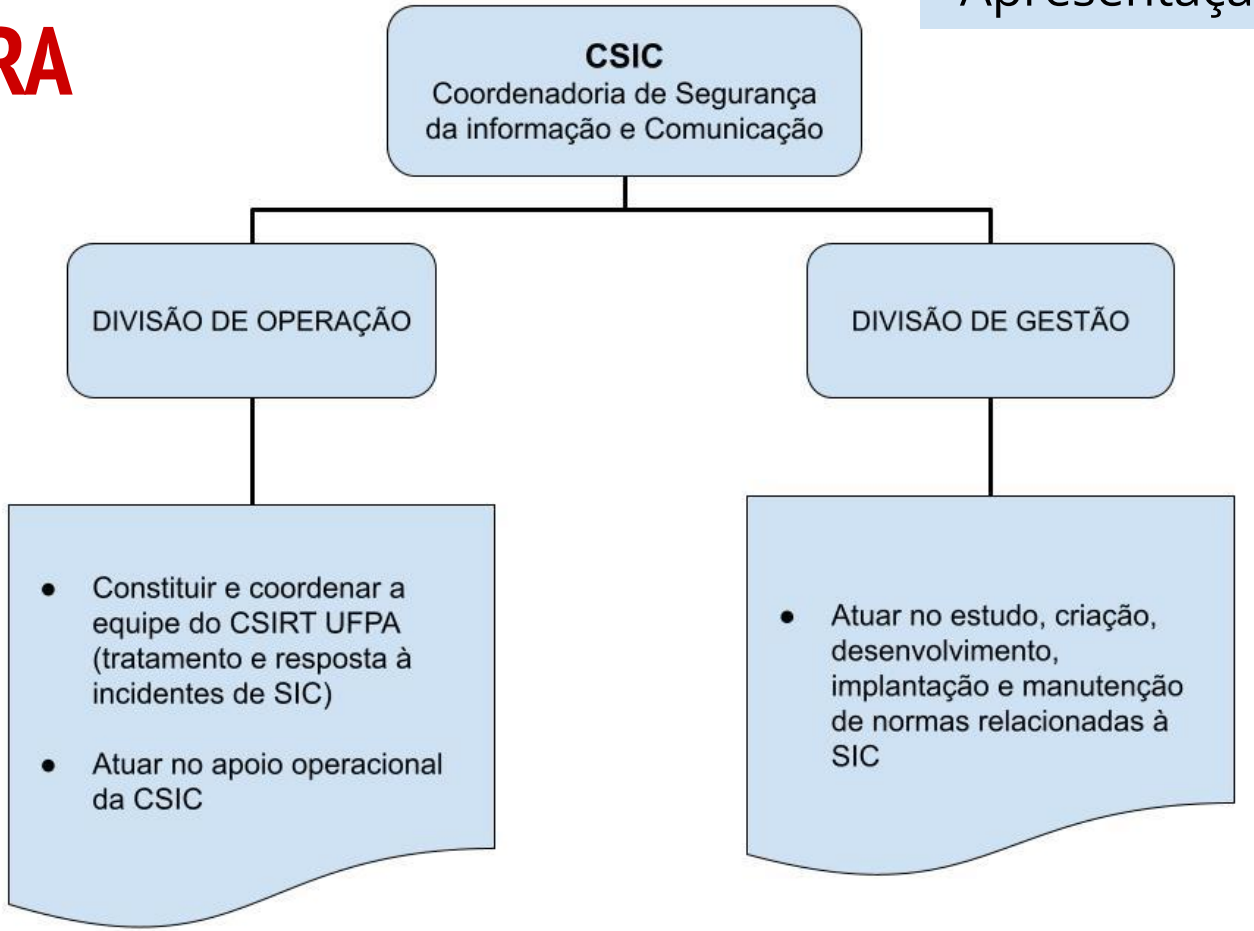
Tanto na área operacional com estudo, desenvolvimento, implantação e manutenção de soluções de segurança da informação e comunicação

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

EQUIPE

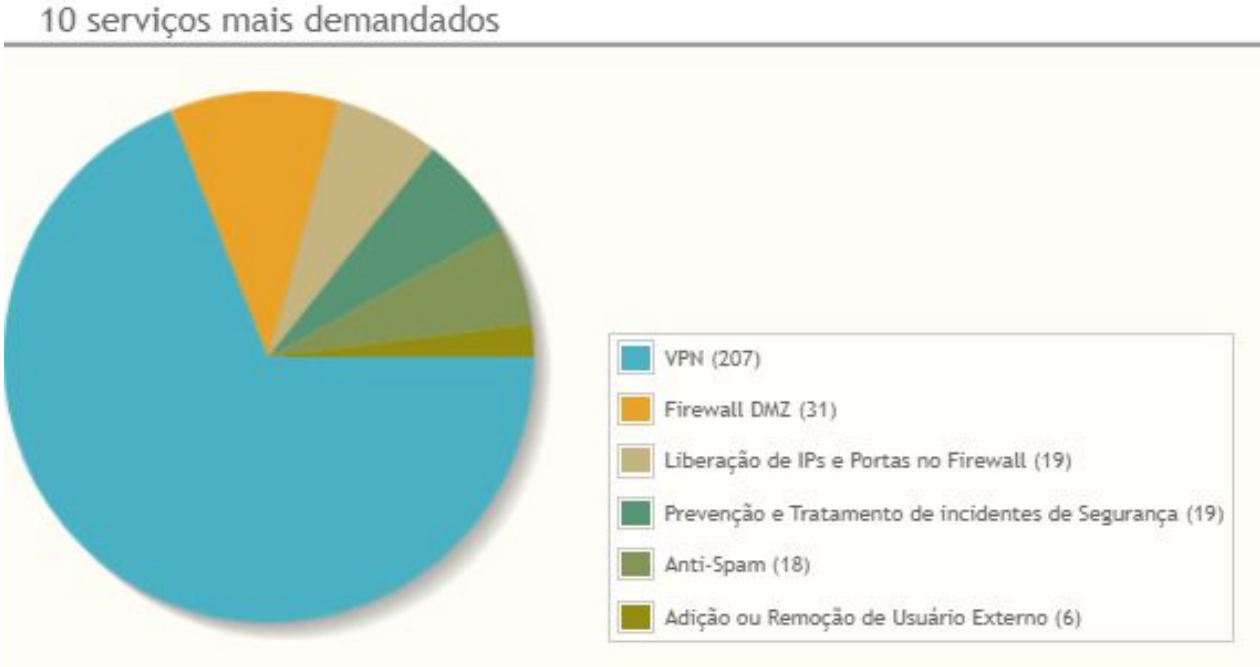
- Rômulo Pinto de Albuquerque - Coordenador CSIC
- Jéssica Janile Monteiro de Castilho - Chefe Div. Gestão
- Jean Carlos Felix de Freitas - Chefe Div. Operação
- Bolsistas:
  - Danilo Ren Nicioka
  - Elienai da Costa Soares

ESTRUTURA


CSIC
Coordenadoria de Segurança da informação e Comunicação
DIVISÃO DE OPERAÇÃO
DIVISÃO DE GESTÃO
Constituir e coordenar a equipe do CSIRT UFPA (tratamento e resposta à incidentes de SIC)
Atuar no apoio operacional da CSIC
Atuar no estudo, criação, desenvolvimento, implantação e manutenção de normas relacionadas à SIC

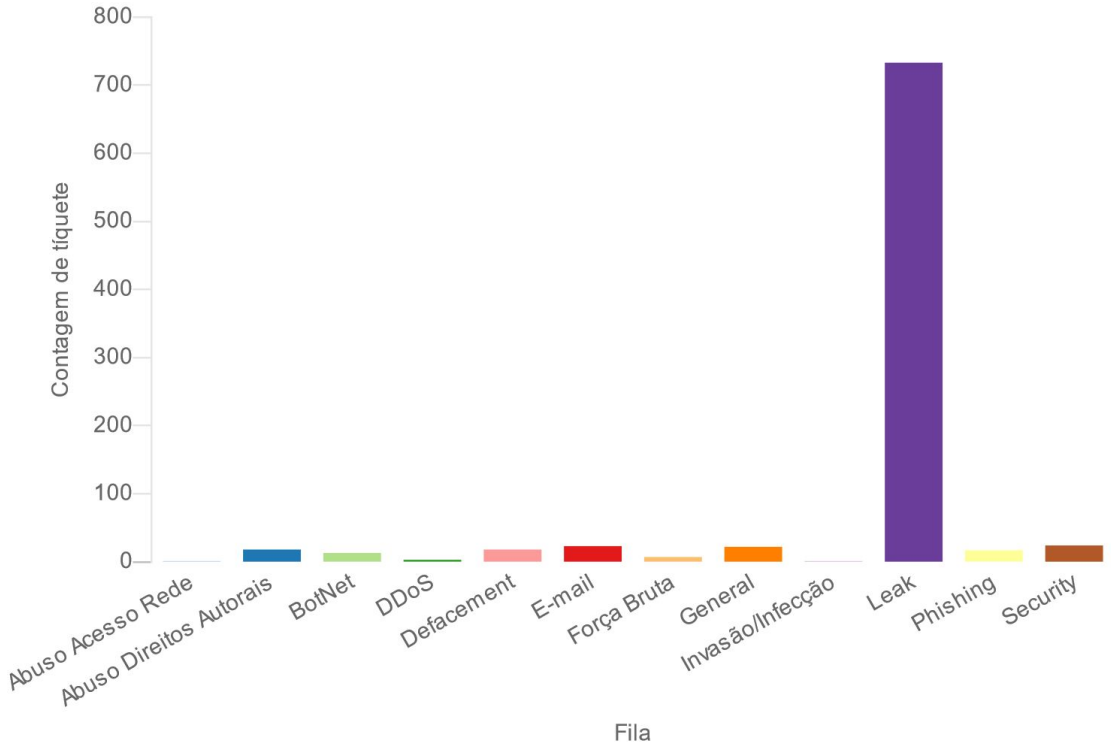
SAGITTA

- **Chamados abertos: 281**
- **Chamados atendidos: 281**



CSIRT - Request Tracker

Atividades ano 2022



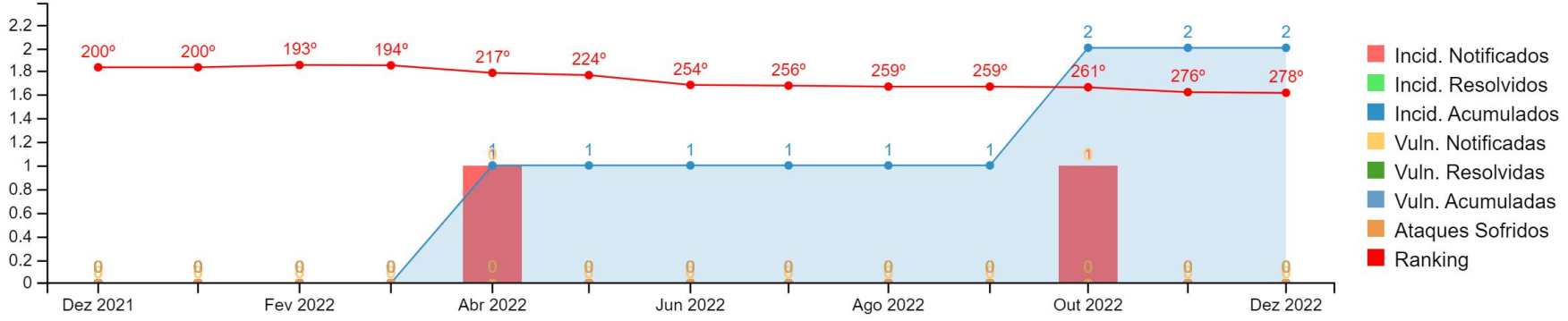
Fila	Contagem de tíquete
Abuso Acesso Rede	1
Abuso Direitos Autorais	18
BotNet	13
DDoS	3
Defacement	18
E-mail	23
Força Bruta	7
General	22
Invasão/Infecção	1
Leak	733
Phishing	17
Security	24
Total	880

CSIRT - SGIS RNP

Atividades ano 2022

Histórico até Dezembro - 2022

12 meses anteriores



AXUR - Vazamento de dados

AXUR INFORMATION SECURITY

Vazamento de Dados

Filtrar Buscar ticket

Abertos 4.749 **Incidentes** 6.482 Tratamento 2 Encerrados 0

UFPA.BR

Para o domínio **ufpa.br**, encontramos em **Janeiro**:

- 1906 credencial(is) vazada(s)

TOTAL DE VAZAMENTOS = **11.233**

WAZUH - Gestão de vulnerabilidades

25 servidores rede DMZ

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

NORMATIVOS

- Política de controle de acesso
- Política de gestão de incidentes
- Plano de gestão de riscos de TI
- Plano de continuidade de negócios de TI

https://governancadigital.ufpa.br/

CURSOS E PALESTRAS

- CAPACIT
  - Boas práticas de segurança da informação na UFPA
  - 04/05 - 08/05/2022

2021

Status PDTIC 2021-2023

ID da ação	Descrição	Prazo	Ano	Status	Percentual de execução	Nível do Risco
A119	Capacitar os servidores na área de segurança da informação para aplicarem ações de prevenção e detecção de incidentes nos seus processos de trabalho	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A122	Realizar monitoramento de todo o tráfego de entrada e saída da rede institucional, através das ferramentas de coleta de logs, e aplicação de técnicas para diagnosticar possíveis ataques cibernéticos	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A123	Implementar políticas de segurança da informação em caráter emergencial ou de forma definitiva para garantir a utilização normal da rede institucional pela comunidade acadêmica da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A124	Confeccionar documento sobre o monitoramento de incidentes, correções, acessos e tráfego na rede institucional	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A125	Disponibilizar acesso a rede institucional ou aos serviços de TIC através de uma conexão VPN (Virtual Private Network) para todos os servidores da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A126	Realizar os procedimentos de atualização, configuração e backup do sistema operacional e features dos firewalls institucionais, habilitar ou desabilitar funcionalidades e usuários com privilégios de acesso	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A127	Implementar regras de firewall para liberar ou negar acessos a determinados serviços e portas, redes ou endereços IP de dentro ou fora dos domínios da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A129	Criação de uma equipe de servidores de TI capacitados para atuarem na prevenção e resolução de incidentes de segurança da informação dentro de seus ambientes de trabalho	Dezembro	2021	Concluído	100,00%	Risco Alto
A130	Criação de um portal web de referência na UFPA sobre assuntos relacionados à segurança da	Dezembro	2021	Concluído	100,00%	Risco Médio

https://csirt.ufpa.br

OFÍCIO-CIRCULAR Nº 01/2021 (28/12)

2021

CSIRT - UFPA

Página inicial | Dicas e Tutoriais | Noticias | Documentos | O que é o CSIRT UFPA

SIRT

Grupo de resposta a incidentes de segurança UFPA

Apresentação | Organizacional | Serviços | Equipe | Contato

meu gov.br

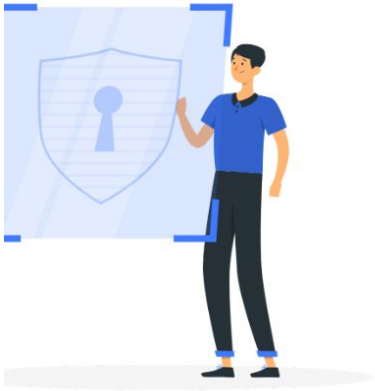
Vazamento expõe dados de milhares de brasileiros

Tweets by CTIC_UFPA

LGPD

Lei Geral de Proteção de Dados

Dicas e Tutoriais



- VPN - SSL e IPSec
- Configurações de Segurança no Windows 10
- Antivírus
- Criptografia - Email e Dados
- Gerenciador de Senhas
- Autenticação de Dois Fatores
- Vazamentos de Dados
- Descarte de Informações em Segurança
- GSuite - UFPA
- Backup do Email Gsuite UFPA
- OCS Inventory NG
- Resolução de Problemas

2022

ID da ação	Descrição	Prazo	Ano	Status	Percentual de execução	Nível do Risco
A118	Implantar um serviço de TI para o inventário de hardware e software para toda a comunidade acadêmica da UFPA	Abril	2022	Concluído	100,00%	Risco Médio
A119	Capacitar os servidores na área de segurança da informação para aplicarem ações de prevenção e detecção de incidentes nos seus processos de trabalho	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A122	Realizar monitoramento de todo o tráfego de entrada e saída da rede institucional, através das ferramentas de coleta de logs, e aplicação de técnicas para diagnosticar possíveis ataques cibernéticos	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A123	Implementar políticas de segurança da informação em caráter emergencial ou de forma definitiva para garantir a utilização normal da rede institucional pela comunidade acadêmica da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A124	Confeccionar documento sobre o monitoramento de incidentes, correções, acessos e tráfego na rede institucional	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A125	Disponibilizar acesso a rede institucional ou aos serviços de TIC através de uma conexão VPN (Virtual Private Network) para todos os servidores da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A126	Realizar os procedimentos de atualização, configuração e backup do sistema operacional e features dos firewalls institucionais, habilitar ou desabilitar funcionalidades e usuários com privilégios de acesso	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A127	Implementar regras de firewall para liberar ou negar acessos a determinados serviços e portas, redes ou endereços IP de dentro ou fora dos domínios da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Alto

2023

ID da ação	Descrição	Prazo	Ano	Status	Percentual de execução	Nível do Risco
A119	Capacitar os servidores na área de segurança da informação para aplicarem ações de prevenção e detecção de incidentes nos seus processos de trabalho	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A120	Realizar procedimentos de teste de invasão para levantar as vulnerabilidades em sistemas, sites, banco de dados e outras soluções de TIC pertencentes a universidade	Março	2023	Em andamento	10,00%	Risco Alto
A121	Implementar correções, em parceria, de vulnerabilidades encontradas pela equipe de pentest, vulnerabilidades informadas pelos fabricantes de soluções de TI ou pela equipe da RNP	Dezembro	2023	Em andamento	30,00%	Risco Alto
A122	Realizar monitoramento de todo o tráfego de entrada e saída da rede institucional, através das ferramentas de coleta de logs, e aplicação de técnicas para diagnosticar possíveis ataques cibernéticos	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A123	Implementar políticas de segurança da informação em caráter emergencial ou de forma definitiva para garantir a utilização normal da rede institucional pela comunidade acadêmica da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A124	Confeccionar documento sobre o monitoramento de incidentes, correções, acessos e tráfego na rede institucional	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A125	Disponibilizar acesso a rede institucional ou aos serviços de TIC através de uma conexão VPN (Virtual Private Network) para todos os servidores da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Médio
A126	Realizar os procedimentos de atualização, configuração e backup do sistema operacional e features dos firewalls institucionais, habilitar ou desabilitar funcionalidades e usuários com	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A127	Implementar regras de firewall para liberar ou negar acessos a determinados serviços e portas, redes ou endereços IP de dentro ou fora dos domínios da universidade	Contínuo	Contínuo	Concluído	100,00%	Risco Alto
A128	Registrar e consultar de forma centralizada os logs produzidos pelos principais ativos e serviços de rede dos campi, em conformidade com as instruções normativas vigentes na UFPA e lei do marco civil de internet	Novembro	2023	Em andamento	30,00%	Risco Alto
A131	Implantar um sistema de verificação de vazamento de dados dos usuários de e-mail da UFPA	Junho	2023	Em andamento	10,00%	Risco Médio

CONTÍNUO

2023

Realizar procedimentos de teste de invasão para levantar as vulnerabilidades em sistemas, sites, banco de dados e outras soluções de TIC pertencentes a universidade	Março	2023	Em andamento	10,00%

50%

GESTÃO DE VULNERABILIDADE

WAZUH

tenable

SOC
Security Operation Center

PoC Claro (inicializada)

- serviço de SOC
  - gestão de vulnerabilidades
  - testes de penetração

2023

Registrar e consultar de forma centralizada os logs produzidos pelos principais ativos e serviços de rede dos campi, em conformidade com as instruções normativas vigentes na UFPA e lei do marco civil de internet	Novembro	2023	Em andamento	30,00%

100%

FORTINET

Managed FortiAnalyzer

500 MB tägliches Logvolumen by ENBITCON

- **Implantado**
- **Retenção de logs por 1 ano**

Em conformidade com Marco Civil da Internet

2023

Implantar um sistema de verificação de vazamento de dados dos usuários de e-mail da UFPA	Junho	2023	Em andamento	10,00%

70%

Vazamento de dados

- **Consulta de vazamentos**
- **Notificação**

PESSOAL

- **Perda de 6 bolsistas nos últimos anos**
  - Começou em 2017 com **8**, agora são **2**

- **Atuação dos membros da divisão de gestão na divisão de operaçã**o
  - **Jéssica** atua também nas demandas da divisão de operação
    - Firewall / VPN
    - PoC Tenable
    - OCS inventory

- **Formação de uma equipe de SOC**
  - monitoramento
  - tratamento e resposta à incidentes
  - gestão de vulnerabilidades
  - pentest