Governo do Estado de
RONDÔNIA
SETIC

Coordenadoria Segurança da Informação
RELATÓRIO MENSAL
Agosto/2021

2021

Relatório Mensal - Agosto/2021

Sumário

1. Introdução 3

2. Tráfego de Rede 3

2.1 Consumo por Secretária 4

3. Ataques 5

4. Vulnerabilidades 5

4.1 CONTEXTO DA ANÁLISE DE VULNERABILIDADES 6

4.2 GRÁFICOS 7

4.3 AÇÕES CORRETIVAS 10

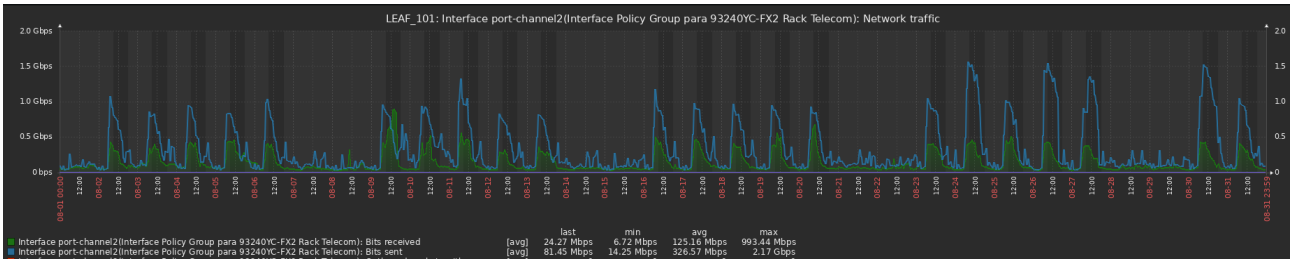
5. Milestones 11

1. Introdução

Está Coordenadoria de Segurança, elaborou este relatório como fins de apresentação de aumento de utilização dos serviços como Redes, Ataques e Vulnerabilidade no mês de Agosto.

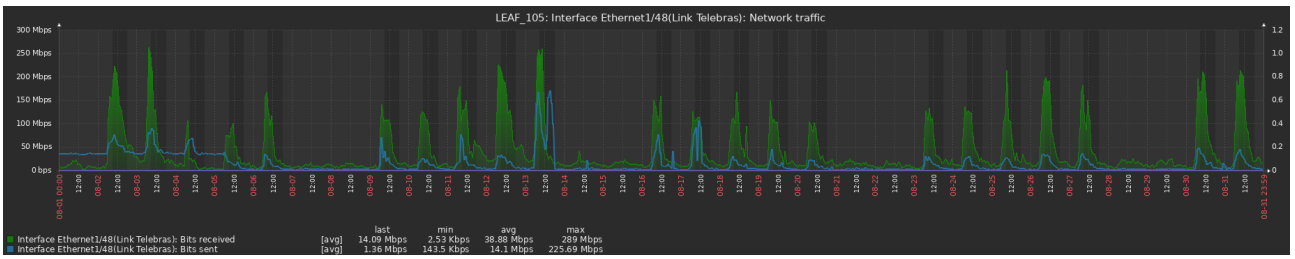
2. Tráfego de Rede

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **151 TB** de informação trafegada no mês deste relatório.

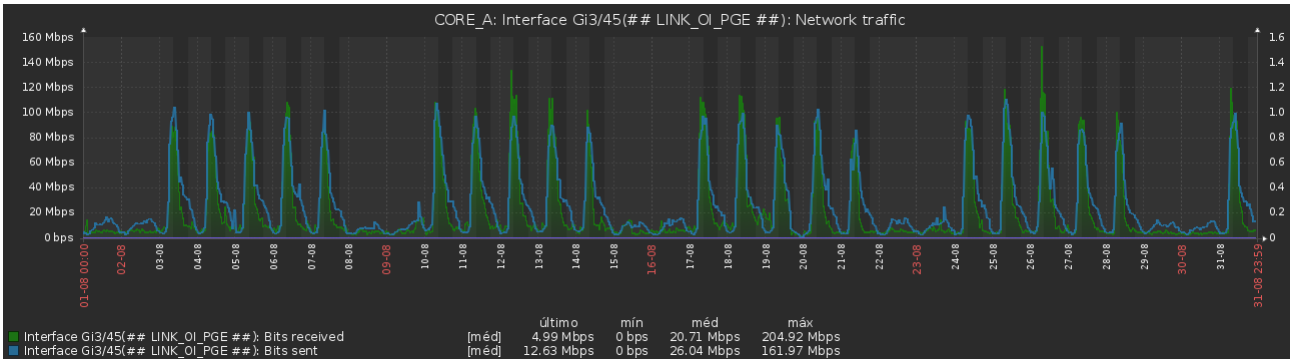


Monitoramento de tráfego Cores SETIC

Além disso, foram consumidos **33 TB** de tráfego da Internet, considerando acesso dos usuários a aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.



Monitoramento de tráfego Cores Link Telebrás



Monitoramento de tráfego Cores Link Oi

2.1 Consumo por Secretária

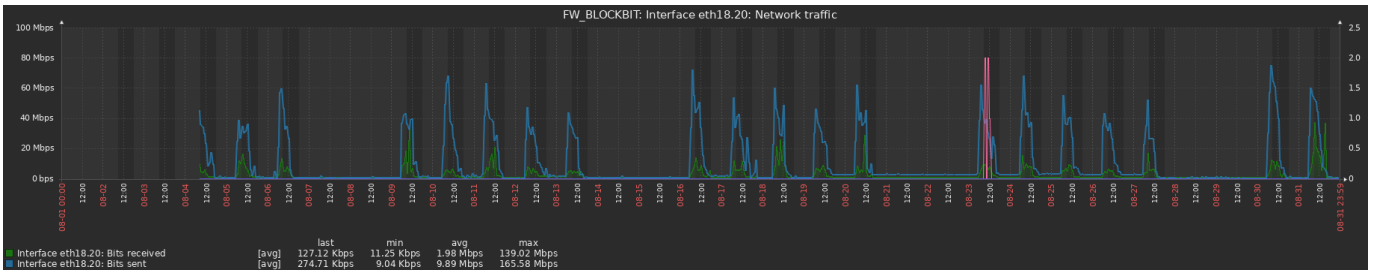
Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **12 TB** de informação trafegada no mês deste relatório por secretaria.

Os dados referem-se às três maiores consumidoras deste mês de Agosto.

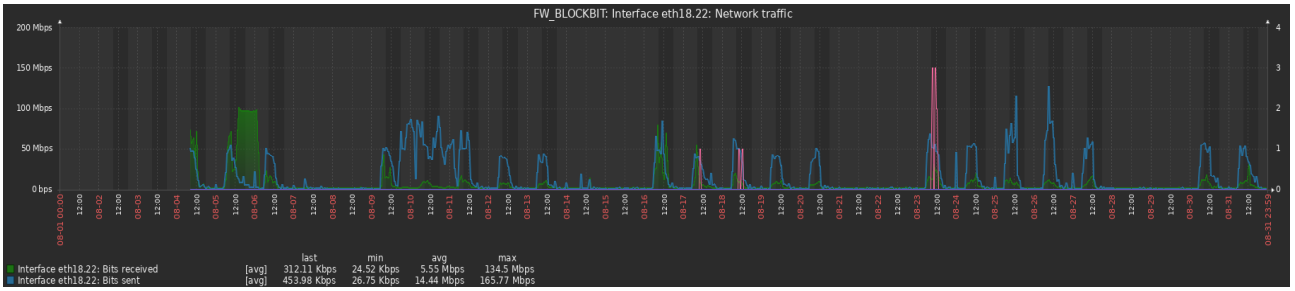
Secretária DER/SEOSP: **4 TB**

Secretária SUGESP: **6 TB**

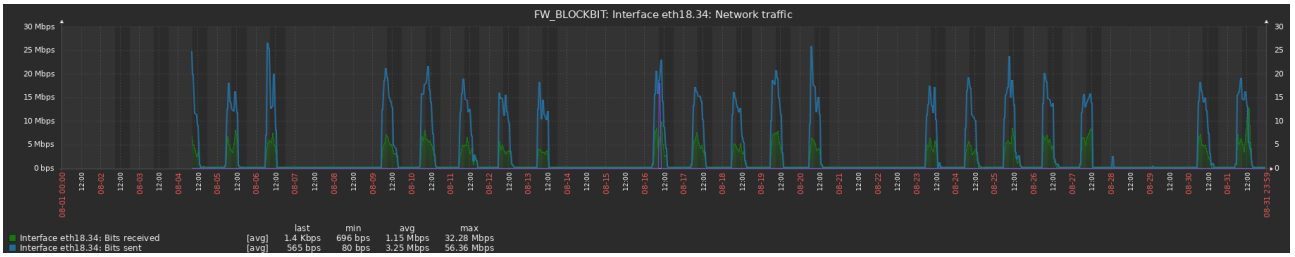
Secretária SEJUCEL: **1 TB**



Monitoramento de tráfego DER/SEOSP



Monitoramento de tráfego SUGESP



Monitoramento de tráfego SEJUCEL

3. Ataques

Vale à pena frisar que ainda não possuímos uma infraestrutura que nos garanta a segurança de dados, no que tange às tecnologias de proteção topo de linha no mercado de TI. Por este motivo, no mês de **Agosto**, a estatística de tentativas de intrusão, para o melhor funcionamento da rede, o serviço foi desabilitado, pois devido alta demanda de consumo, o equipamento disponível não suporta o recurso em nosso ambiente.

4. Vulnerabilidades

Trata-se das reanálises de vulnerabilidades realizadas sem servidores de rede pertencentes ao Governo do Estado de Rondônia gerenciados ou hospedados pela SETIC, utilizando-se os softwares Nmap 1 e OpenVAS 2.

Tais procedimentos se deram em decorrência das diretrizes da Coordenação de Segurança da Informação da SETIC, bem como a solicitação da equipe de Data Center da Coordenação de Infraestrutura da SETIC.

O OpenVAS, ao analisar determinado alvo, classifica as vulnerabilidades encontradas em 3 (três) diferentes níveis de gravidade: **alto, médio e baixo**. Destaca-se ainda que apresenta também o nível denominado “log”, que objetiva trazer informações sobre o alvo, não sendo objeto de discussão neste relatório.

Ao todo, foram reanalisados **58** (cinquenta e oito) servidores de rede, dos quais **27 (46,6%)** apresentaram **alto** nível de gravidade, **14 (24,1%)** apresentaram **médio** nível, **3 (5,2%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **8 (13,8%)** servidores não apresentaram **nenhuma** vulnerabilidade.

Também encontramos **6 (10,3%)** endereços que não responderam, ou desligados ou inalcançáveis.

Importante ressaltar que nas análises, alguns servidores que apresentaram alto nível de gravidade também apresentaram gravidades de nível médio e baixo, bem como alguns servidores que apresentaram médio nível de gravidade também apresentaram gravidades de nível baixo.

No decorrer das análises o OpenVAS detectou **518 notificações**, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **90 (17,4%)** de **alto** nível, **384 (74,1%)** de **médio** nível e **44 (8,5%)** de **baixo** nível.

Nos testes realizados foram identificadas diversas vulnerabilidades, entretanto não se descarta outras que por ventura não foram detectadas ou que surjam futuramente.

4.1 CONTEXTO DA ANÁLISE DE VULNERABILIDADES

Considerando as novas diretrizes da Coordenação de Segurança da Informação da SETIC, a solicitação da equipe de Data Center da Coordenação de Infraestrutura da SETIC, realizou-se as análises nos seguintes hosts:

172.16.1.24 - 172.16.1.25 - 172.16.1.251 - 172.16.1.252 - 172.16.1.253 - 172.16.1.254 - 172.16.1.36 - 172.16.1.37 - 172.16.1.44 - 172.16.1.45 -

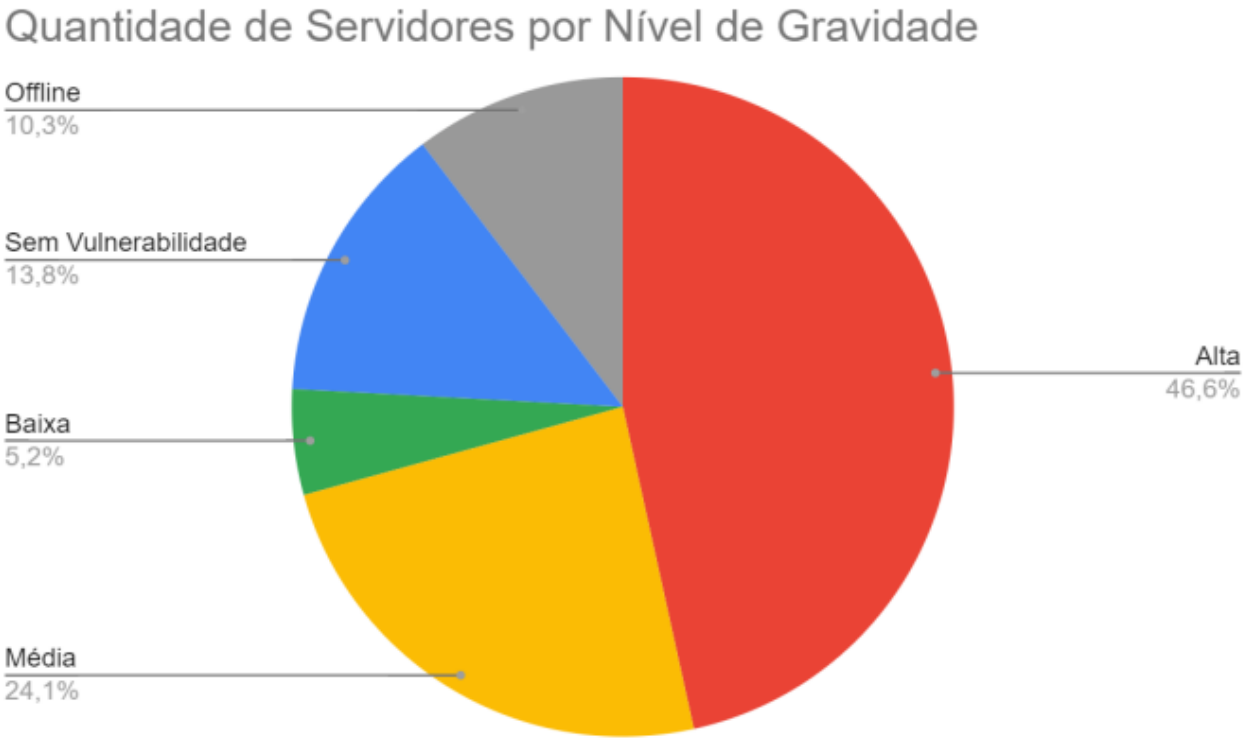
172.16.1.99 - 172.16.107.192 - 172.16.111.5 - 172.16.111.7 - 172.16.111.9 - 172.16.112.10 - 172.16.112.11 - 172.16.112.2 - 172.16.112.9 - 172.16.123.136 - 172.16.130.130 - 172.16.130.131 - 172.16.132.10 - 172.16.132.11 - 172.16.132.14 - 172.16.139.16 - 172.16.139.39 - 172.16.139.42 - 172.16.139.43 - 172.16.16.2 - 172.16.16.3 - 172.16.16.4 - 172.16.200.44 - 172.16.28.10 - 172.16.28.11 - 172.16.28.5 - 172.16.28.6 - 172.16.28.8 - 172.16.28.9 - 172.16.36.2 - 172.16.36.3 - 172.16.47.131 - 172.16.47.135 - 72.16.47.136 - 172.16.6.133 - 172.16.6.134 - 172.16.6.142 - 172.16.6.143 - 172.16.6.152 - 172.16.6.153 - 172.16.6.155 - 172.16.6.156 - 172.16.6.165 - 172.16.6.166 - 172.16.6.167 - 172.16.6.168 - 172.16.6.21 - 201.11.159.22

Nesse sentido, primeiro foi iniciada a etapa de levantamento de informações e versionamentos, utilizando-se o Nmap. Logo em seguida, utilizou-se um software de análise de vulnerabilidade genérico, OpenVAS.

4.2 GRÁFICOS

Utilizando-se do OpenVAS, considerando sua classificação das vulnerabilidades em 3 (três) diferentes níveis de gravidade (**alto, médio e baixo**) foi possível re-analisar **58** (cinquenta e oito) servidores de rede, dos quais **27 (46,6%)** apresentaram **alto** nível de gravidade, **14 (24,1%)** apresentaram **médio** nível, **3 (5,2%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **8 (13,8%)** servidores não apresentaram **nenhuma** vulnerabilidade, também encontramos **6 (10,3%)** endereços que não responderam, ou desligados ou inalcançáveis, conforme “Gráfico 1 – Nível de gravidade” abaixo:

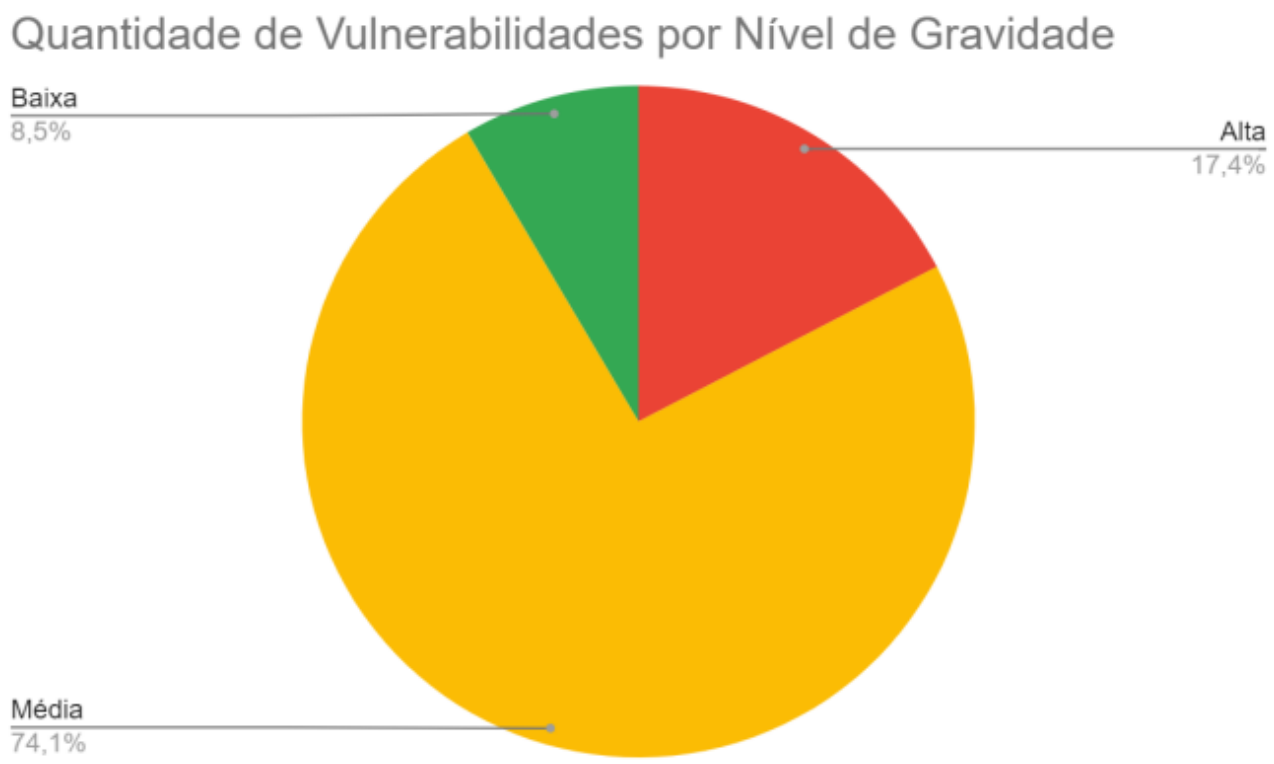
Gráfico 1 - Nível de gravidade.



Fonte: Próprio autor (2021), com base nos relatórios de vulnerabilidade do OpenVAS.

No que diz respeito às notificações apresentadas pelo OpenVAS, destacam-se que foram detectadas **518** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **90 (17,4%)** de **alto** nível, **384 (74,1%)** de **médio** nível e **44 (8,5%)** de **baixo** nível, conforme “Gráfico 2 – Total de notificações” abaixo:

Gráfico 2 - Total de notificações

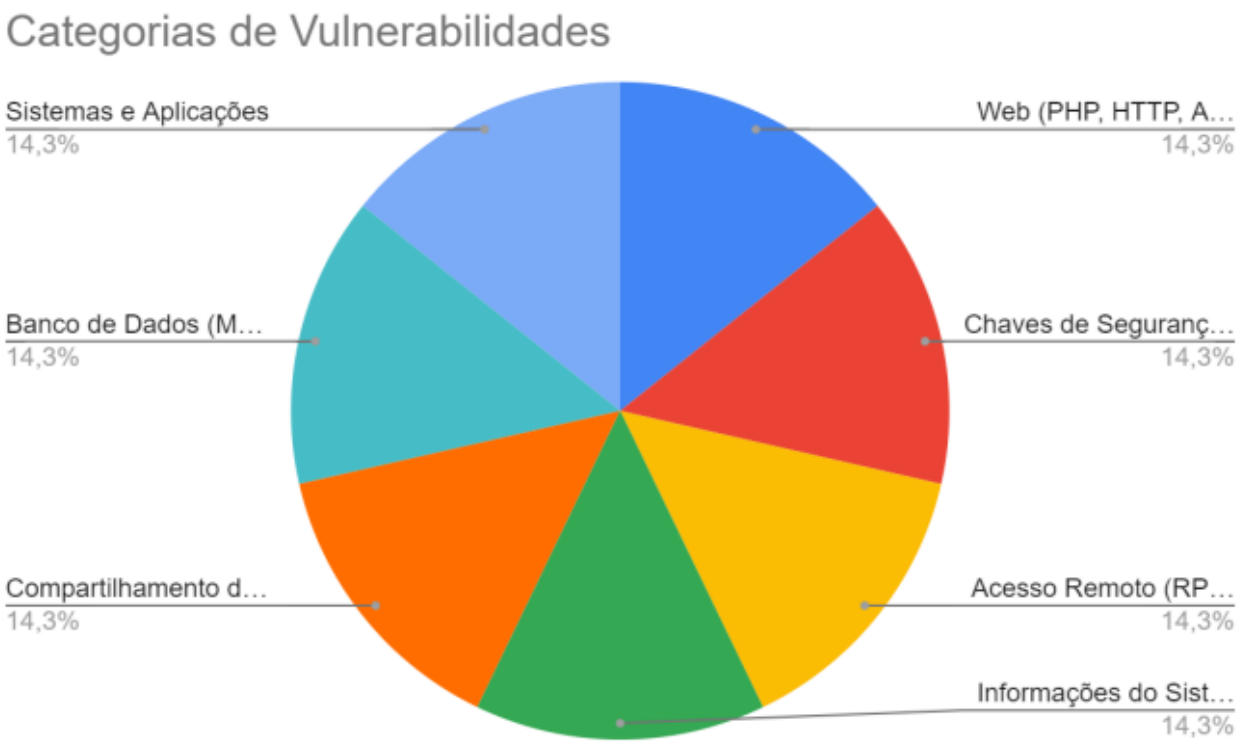


Fonte: Próprio autor (2021), com base nos relatórios de vulnerabilidade do OpenVAS.

Além disso, com base nos relatórios do OpenVAS, procurou-se categorizar as principais vulnerabilidades encontradas nos servidores de rede que foram analisados, criando as seguintes categorias: Web (PHP, HTTP, APACHE), Chaves de Segurança (SSL, TLS, OPENSSH), Acesso Remoto (RPC, FTP, DCE, TCP), Informações do Sistema (TCP TIMESTAMPS), Compartilhamento de Arquivos (Backup, SMB), Banco de Dados (MariaDB, SQL), Sistemas e Aplicações.

Dessa forma, procurou-se destacar a vulnerabilidade mais crítica de cada servidor e classificá-la em uma dessas categorias, com objetivo de facilitar a identificação do segmento que se encontra mais vulnerável na rede, exigindo atenção e adoção de políticas de correção e mitigação de falhas e problemas de segurança. Sendo assim, foi possível perceber que a maioria das vulnerabilidades encontradas estão vinculadas à WEB (33 servidores), Chaves de Segurança (42 servidores) e Informações do Sistema (46 servidores), conforme observado no “Gráfico 3 – Categorias de vulnerabilidades” abaixo:

Gráfico 3 - Categorias de Vulnerabilidade.



Fonte: Próprio autor (2021), com base nos relatórios de vulnerabilidade do OpenVAS.

4.3 AÇÕES CORRETIVAS

Após a realização das análises e produção dos relatórios, contendo informações conjuntas do Nmap e OpenVAS, estes foram enviados ao setor de Data Center, responsável por realizar as correções aplicando as medidas necessárias. Tal procedimento foi determinado pela Coordenação de Segurança da Informação da SETIC, considerando que esse setor que administra os servidores que foram analisados.

Os relatórios foram enviados por meio de chamados abertos pelo GLPI (https://atendimento.detic.ro.gov.br/), sistema de controle de requisições da SETIC, sob os protocolos de número:

2021090065 - 2021090069 - 2021090071 - 2021090072 - 2021090073 - 2021090074 - 2021090075 - 2021090076 - 2021090078 - 2021090080 - 2021090081 - 2021090709 - 2021090712 - 2021090713 - 2021090714 - 2021090715 - 2021090717 - 2021090718 - 2021090356 - 2021090719 - 2021090720 - 2021090723 - 2021090728 - 2021090729 - 2021041135 - 2021091207 - 2021091208 - 2021091209 - 2021091263 - 2021091266 - 2021091269 - 2021091271 - 2021091272 - 2021091274 - 2021091275 - 2021091276 - 2021091279 - 2021091281 - 2021091282 - 2021091285 - 2021092288 - 2021092289 - 2021092290 - 2021092292 - 2021092293 - 2021092294 - 2021092295 - 2021092297 - 2021092300 - 2021092302 - 2021092304 - 2021092307 - 2021092309

Controle de análises, encontra-se uma tabela contendo informações sobre as referências, endereços de IP, datas das análises, softwares utilizados para realizá-las, nível de gravidade, as principais falhas detectadas, a vinculação de endereços internos ou externos quando identificados, o número do chamado no GLPI e sua data de abertura.

5. Milestones

Descrição dos principais projetos que impactaram nessa coordenação, com impactos positivos na sua implementação e que influencia nos bons resultados para fins de segurança.

Segue dois milestones:

Milestone 1:

Data:	Identificação
01.08.2021	Implementação do Firewall CTN
Descrição:	Implementação do Firewall no ambiente de Datacenter do Container SETIC. Este equipamento é responsável por fazer o filtro de conexões de entrada e saída entre as redes dos serviços hospedados no ambiente e a internet.
Resultado:	Implementação de funcionalidades de segurança e recursos de auditoria através de análise de logs e geração de relatórios.

Milestone 2:

Data:	Identificação

25.08.2021	Troca de Firewall da INFOVIA
Descrição:	Substituição de Firewall com limitação de recursos operacionais por novo Firewall com melhor disponibilidade de funcionalidades e suporte técnico por parte do fabricante. Este equipamento é responsável por fazer o filtro de conexões de entrada e saída entre as redes interconectadas pela infraestrutura da INFOVIA.
Resultado:	Aumento do canal de tráfego de dados na comunicação por conta da melhoria de desempenho do novo equipamento. Solução de problemas de limite de usabilidade através da implementação de novas funcionalidades de segurança. Novos recursos de auditoria através de análise de logs e geração de relatórios.

Superintendência do
Estado para Resultados

Governo do Estado de
RONDÔNIA