Governo do Estado de
RONDÔNIA
SETIC

Coordenadoria de Segurança
RELATÓRIO MENSAL
Maio/2021

2021

Relatório Mensal - Maio/2021

Sumário

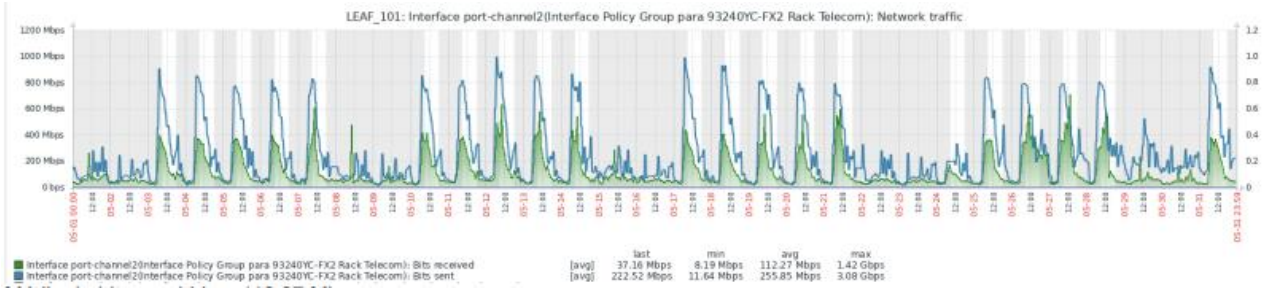
1. Introdução

Está coordenadoria de Segurança, elaborou este relatório como fins de apresentação aumento de utilização dos serviços como Redes, Ataques e Vulnerabilidade. Acrescentando os últimos dois meses anteriores deste mês de maio.

2. Tráfego de Rede

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da DETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **123 TB** de informação trafegada no mês deste relatório.

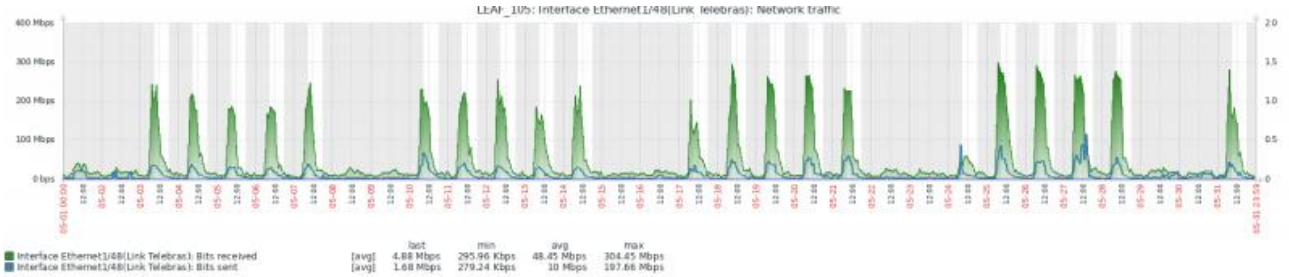
Salientamos que comparando os meses interiores teve um aumento **18,69%** de consumo.



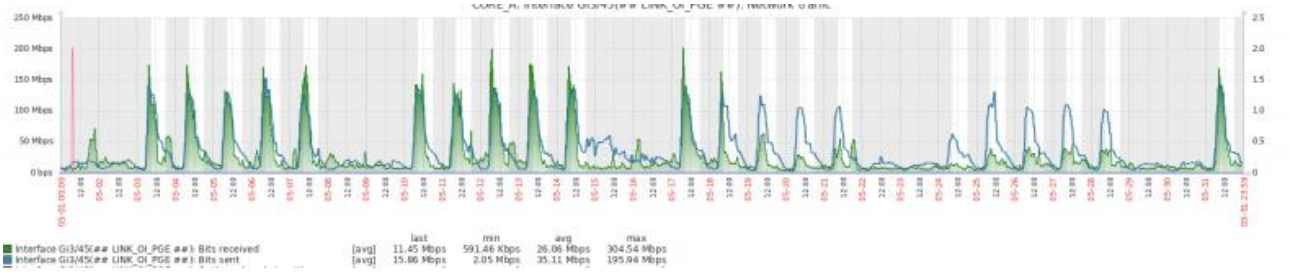
Monitoramento de tráfego Cores DETIC

Além disso, foram consumidos **40 TB** de tráfego da Internet, considerando acesso dos usuários à aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.

Salientamos que comparando os meses interiores teve um aumento **2,5%** de consumo.



Monitoramento de tráfego Link Telebrás



Monitoramento de tráfego Link Oi

2.1 Consumo por Secretária

Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da DETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **11,7 TB** de informação trafegada no mês deste relatório por secretária.

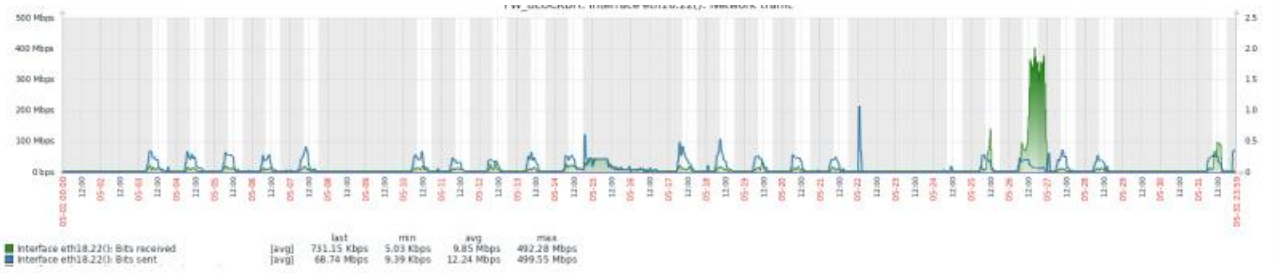
Dados refere-se as duas mais consumidoras deste mês.

Secretária DER/SEOSP: **3 TB**

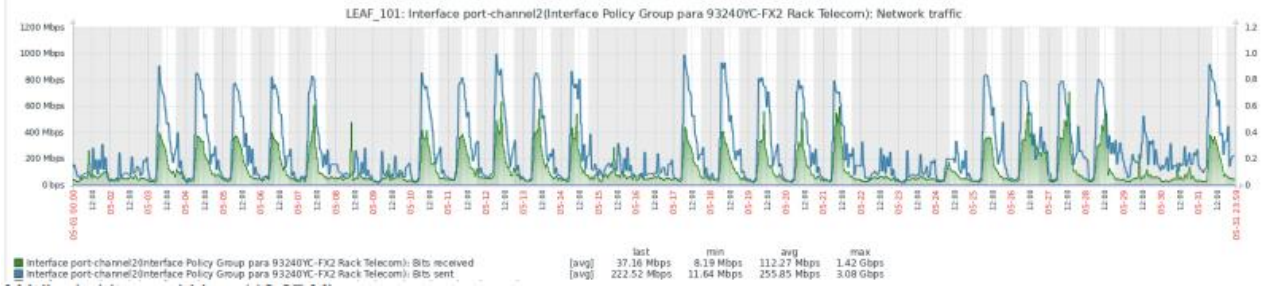
Secretária SUGESP: **7 TB**

Secretária SEGEP: **1,7 TB**

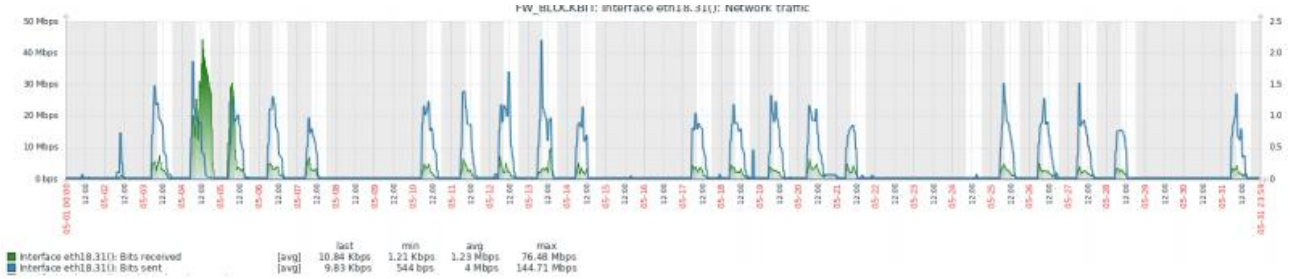
Salientamos que comparando os meses interiores teve um aumento **95%** de consumo.



Monitoramento de tráfego DER/SEOSP



Monitoramento de tráfego SUGESP



Monitoramento de tráfego SEGEP

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 o mês de ***Maio***, 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.

Usando comparação dos dois meses anteriores somando os ataques totalizando: **113,590.**

4. Vulnerabilidades

Trata-se das análises de vulnerabilidades realizadas em 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 da intenção de criar a Gerência de Prevenção e Respostas a Incidentes e a solicitação das equipes de Operações e DataCenter 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 nesse trimestral (Março, Abril e Maio) foram analisados **78 (Setenta e Oito)** servidores de rede, dos quais **20 (26%)** apresentaram **alto** nível de gravidade, **39 (50%)** apresentaram **médio** nível, **12 (15%)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **7 (9%)** servidores não apresentaram **nenhuma vulnerabilidade**, pelo fato de estarem com todas as portas fechadas.

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 **606 notificações**, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **34 (9 %) de alto nível, 501 (47 %) de médio nível e 71 (44 %) de baixo nível.**

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

4.1 Quantidade de Servidores

Utilizando-se do OpenVAS, considerando sua classificação das vulnerabilidades em 3 (três) diferentes níveis de gravidade (alto, médio e baixo) foi possível analisar **78 (Setenta e O)** servidores de rede, dos quais **20 (26 %)** apresentaram **alto** nível de gravidade, **39 (50 %)** apresentaram **médio** nível, **12 (15 %)** apresentaram **baixo** nível, conforme classificação do OpenVAS, destacando-se ainda que **7 (9 %)** servidores não apresentaram **nenhuma** vulnerabilidade, pelo fato de estarem com todas as portas fechadas, conforme "Gráfico 1 – Nível de gravidade" abaixo:

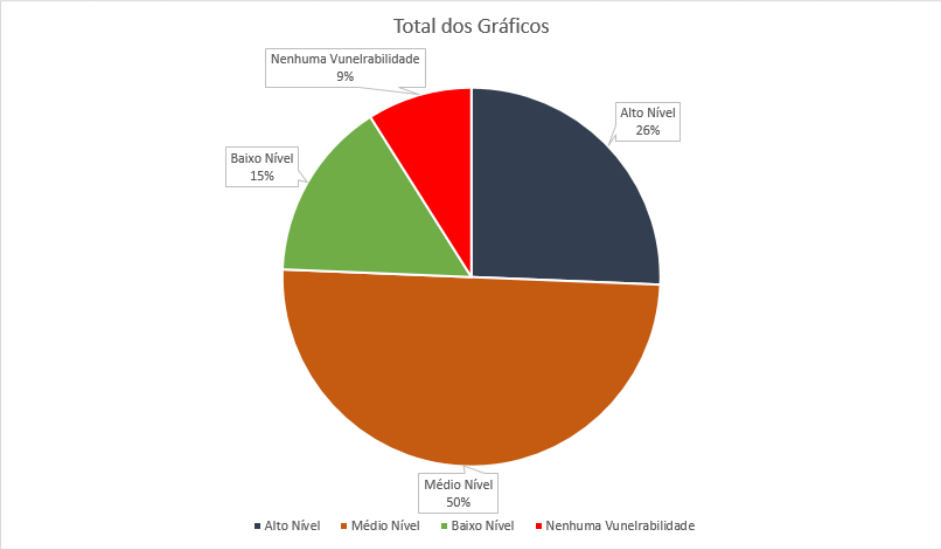


Gráfico 1 – Quantidade de Servidores

4.2 Quantidade de Vulnerabilidades

No que diz respeito às notificações apresentadas pelo OpenVAS, destacam-se que foram detectadas **34 (9 %)** de alto nível, **501 (47 %)** de médio nível e **71 (44 %)** de baixo nível.

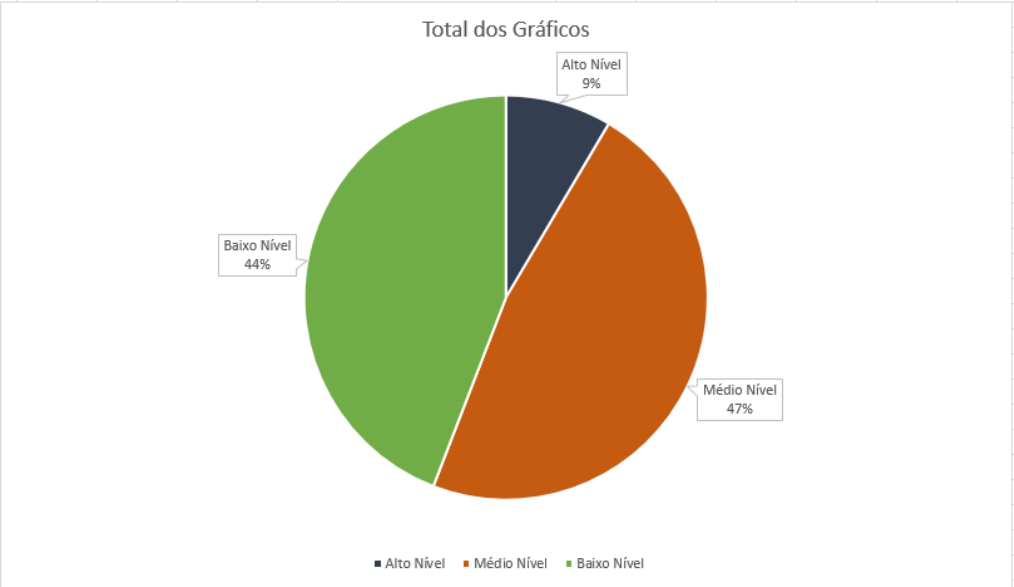


Gráfico 2 – Quantidade de Vulnerabilidade

4.3 Categoria de Vulnerabilidades

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 (SMB WINDOWS); Banco de Dados (MariaDB, SQL); e Backup File. Dessa forma, procurou-se destacar a vulnerabilidade mais crítica de cada servidor e classificála 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 Acesso Remoto **(57 servidores) Chaves de Segurança (51 servidores) e Informações do Sistema (64 servidores).**

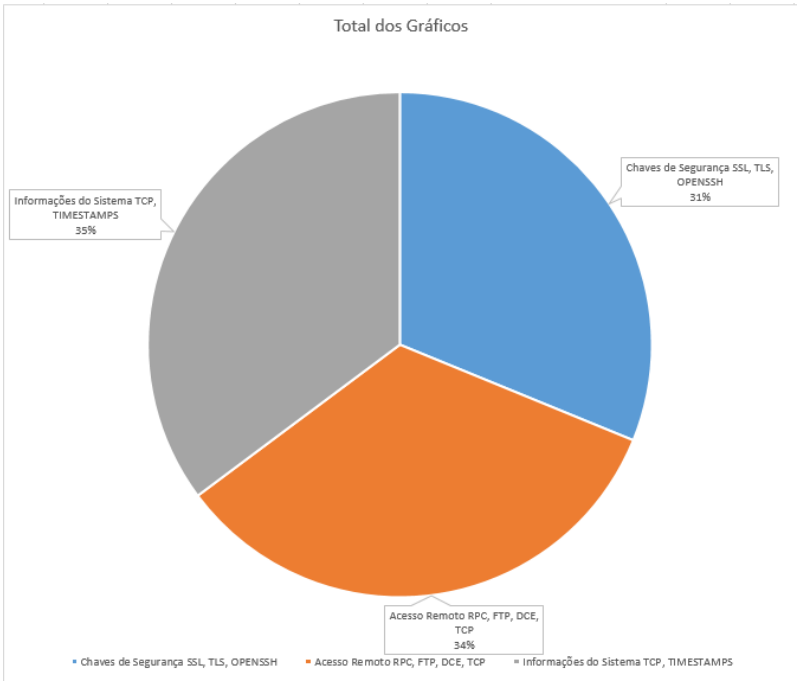


Gráfico 3 – Categoria de Vulnerabilidades

Superintendência do
Estado para Resultados

Governo do Estado de
RONDÔNIA

Wiki.DETIC

Plataforma de Documentação Operacional e Gerencial dos Serviços da EpR

Conheça: wiki.detic.ro.gov.br