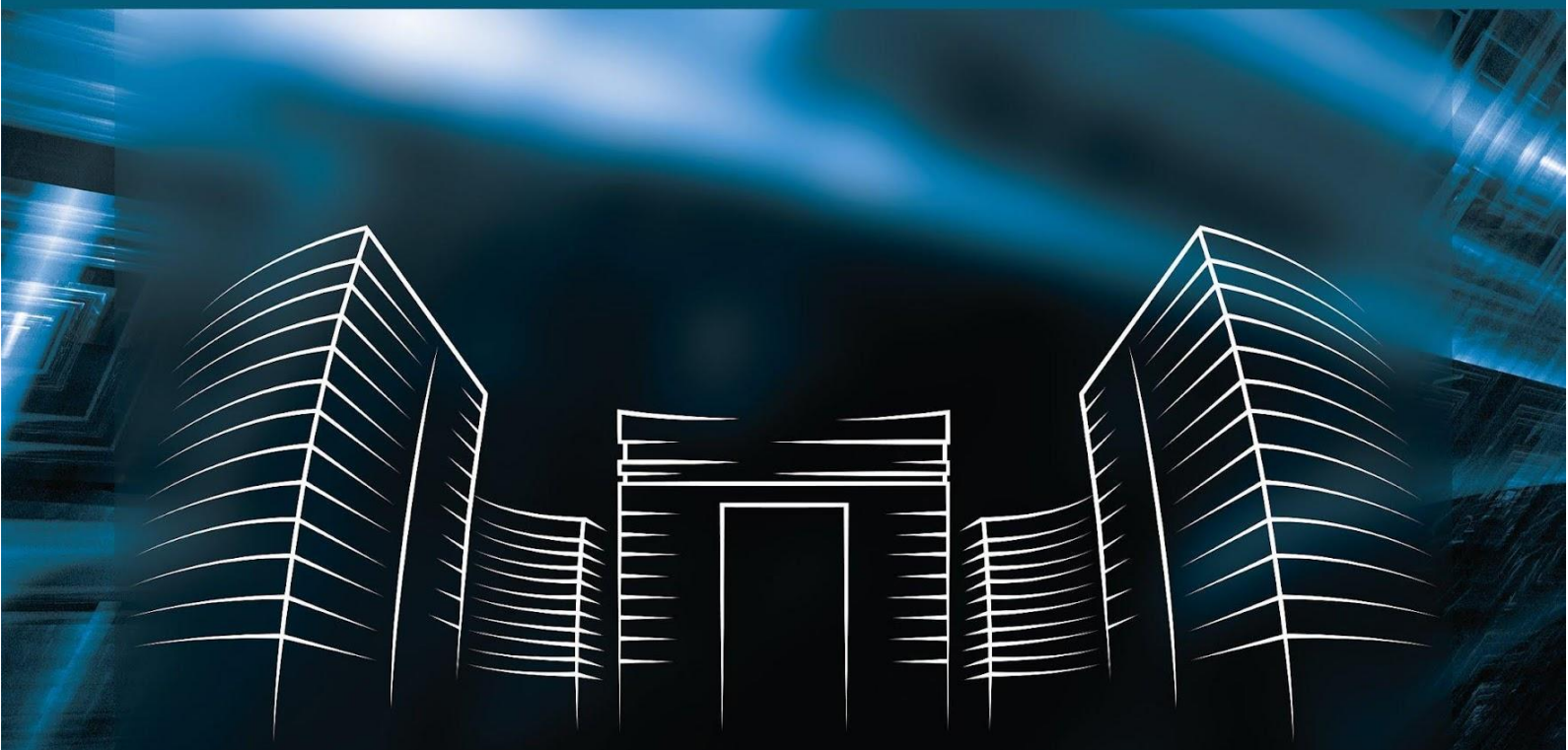
SETIC
Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

RELATÓRIO FEVEREIRO/2022

COSEGI



2022

GOVERNO DO ESTADO DE RONDÔNIA

Cel. Marcos José Rocha dos Santos

Governador

José Atilio Salazar Martins

Vice-Governador

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Cel. Delner Freire

Superintendente

Maico Moreira Silva

Diretor Técnico

COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Leonardo Courinos Lima da Silva

Coordenador

ELABORAÇÃO

Rosemeire Vidal da Silva

REVISÃO

Leonardo Courinos Lima da Silva

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	28/02/2022	Rosemeire Vidal, Eduardo Zimmer, Rogério Eduardo e Leonardo Courinos.	Elaboração do relatório.

LISTA DE ABREVIATURAS

SETIC Superintendência Estadual de Tecnologia da Informação e Comunicação

COSEGI Coordenadoria de Segurança da Informação

INFOVIA Interligar unidades organizacionais do poder público por meio de uma rede de alta disponibilidade e velocidade.

WAF Firewall de Aplicação Web

IPS Sistema de Prevenção de Intrusão

OSSIM Open Source Security Information Management

GLPI Gestionnaire Libre de Parc Informatique (Gestor de Equipamentos de TI de Código Aberto).

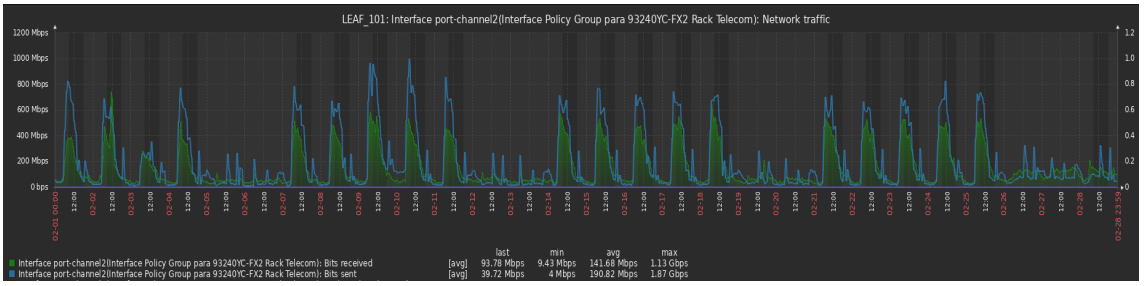
SUMÁRIO

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 fevereiro.

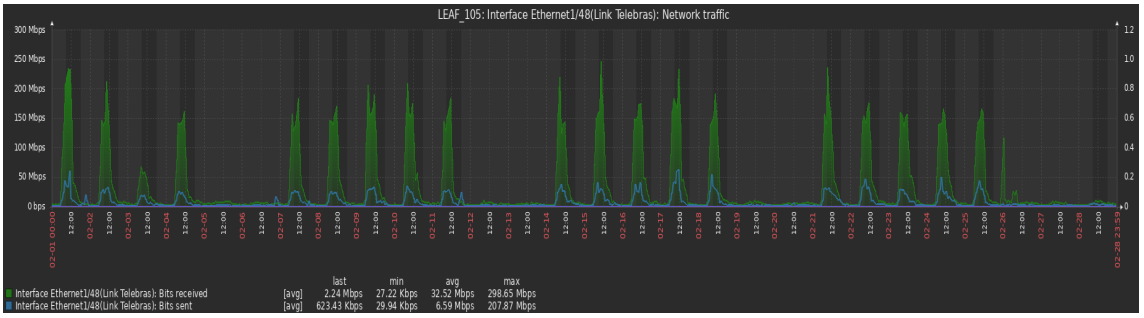
2 TRÁFEGO DE REDE

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 **149 TB** de informação trafegada no mês deste relatório.

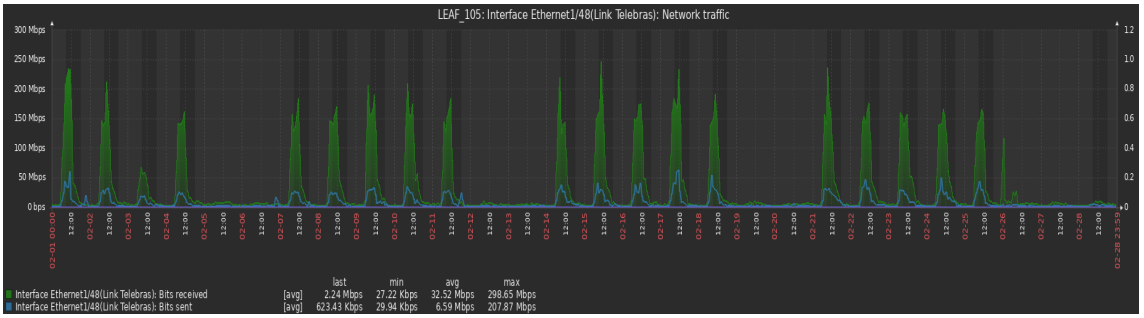


Monitoramento de tráfego Cores SETIC

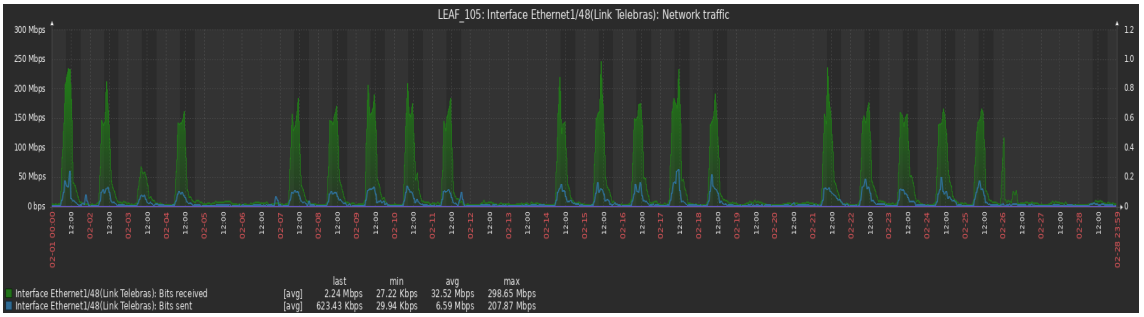
Além disso, foram consumidos **13,09 TB** de tráfego da Internet, considerando acesso dos usuários a aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.



Monitoramento de tráfego Cores Link Telebrás



Monitoramento de tráfego Cores Link Oi - SETIC



Monitoramento de tráfego Cores Link Oi - INFOVIA

2.1 Consumo por Secretaria

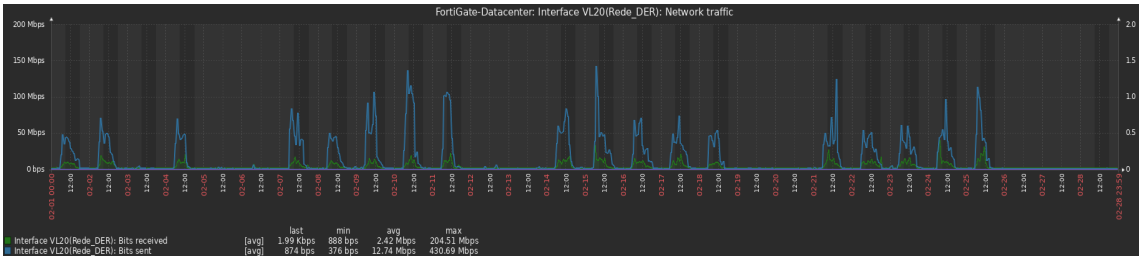
Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **12 TB** de informação trafegada no mês deste relatório por secretaria.

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

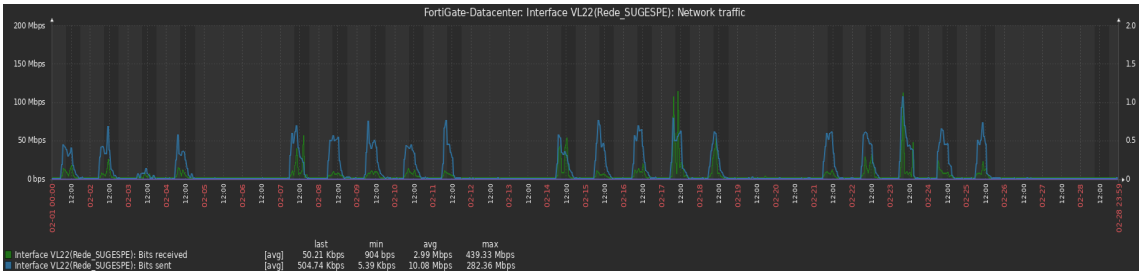
Secretária DER/SEOSP: **5 TB**

Secretária SUGESP: **4 TB**

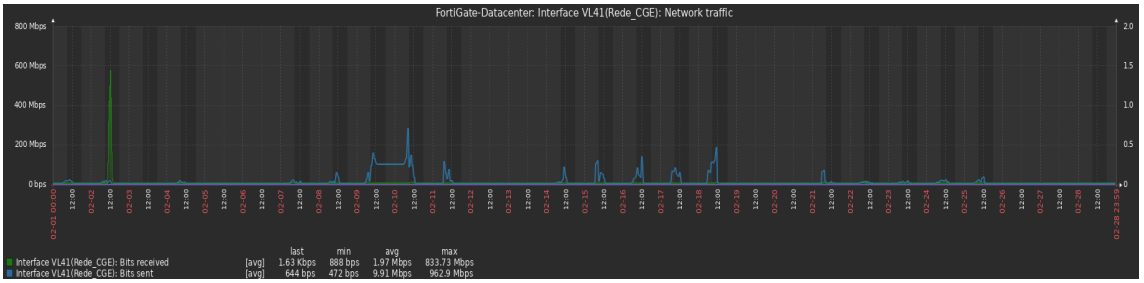
Secretária CGE: **3 TB**



Monitoramento de tráfego DER/SEOSP



Monitoramento de tráfego SUGESP

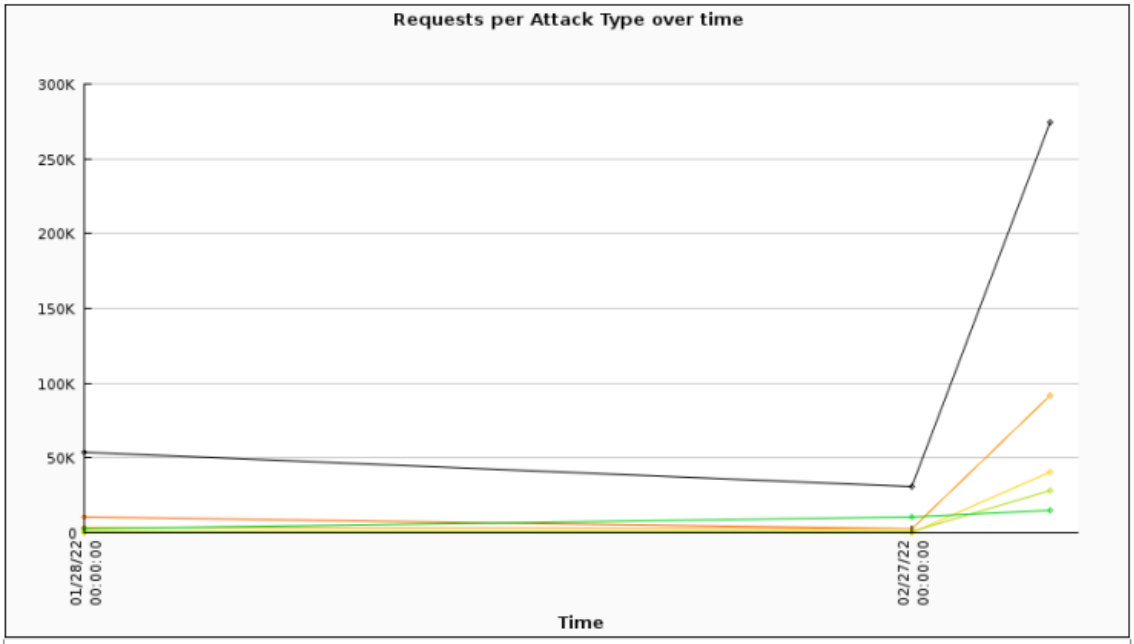


Monitoramento de tráfego CGE

3 ATAQUES

Durante o mês de **Fevereiro** as tentativas de ataques bloqueados através do firewall de aplicação Web (WAF), no qual protege contra ameaças emergentes, foi no total de **302.158** (Trezentos e dois mil, cento e cinquenta e oito) tentativas de ataques. E segue os top 5 tentativas de ataque:

1	Forceful Browsing: 105.284
2	Buffer Overflow: 97.968
3	Session Hijacking: 40.938
4	Abuse of Functionality: 29.079
5	Information Leakage: 28.889



Attack Type	▼ Requests
Forceful Browsing	105284
Buffer Overflow	97968
Session Hijacking	40938
Abuse of Functionality	29079
Information Leakage	28889
Total Attacks count for all requests	360087

Displaying **5** out of total **24** entries

Também foram bloqueadas um total de **416.020** (Quatrocentos e dezesseis mil e vinte) tentativas de intrusões a sistemas e redes da SETIC através do Sistema de Prevenção de Intrusão (IPS), integrado ao Firewall de borda.

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 o software AlienVault OSSIM[1].

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

O OSSIM, ao analisar determinado alvo, classifica as vulnerabilidades encontradas em 4 (quatro) diferentes níveis de gravidade: **crítico, alto, médio** e **baixo**. Destaca-se ainda que apresenta também o nível denominado “info”, que objetiva trazer informações sobre o alvo, não sendo objeto de discussão neste relatório.

Ao todo, foram analisados **70** servidores de rede, dos quais **20 (28,6%)** apresentaram **alto** nível de gravidade, **43 (61,4%)** apresentaram **médio** nível, **4 (5,7%)** apresentaram **baixo** nível, conforme classificação do OSSIM, destacando-se ainda que **1 (1,4%)** servidores não apresentaram **nenhuma** vulnerabilidade.

Também encontramos **2 (2,9%)** 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.

---

[1] é uma solução open source para gerenciamento de eventos de segurança (SIEM-Security Information and Event Management) com inteligência para classificar riscos de eventos e ativos, verificar a conformidade com as normas ISO 27001 e PCI-DSS e gestão de incidentes de segurança, tudo integrado em uma única plataforma. Esta solução é desenvolvida em Python, PHP, XML, AJAX e outras. Ela usa ferramentas como Snort, Nessus, OpenVAS, MySQL, Apache e muitas outras para prover uma solução integrada de monitoramento de eventos.

No decorrer das análises o OSSIM detectou **554** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **36 (6,5%)** de **alto** nível, **391 (70,6%)** de **médio** nível e **127 (22,9%)** de **baixo** nível.

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

5 CONTEXTO DA ANÁLISE DE VULNERABILIDADE

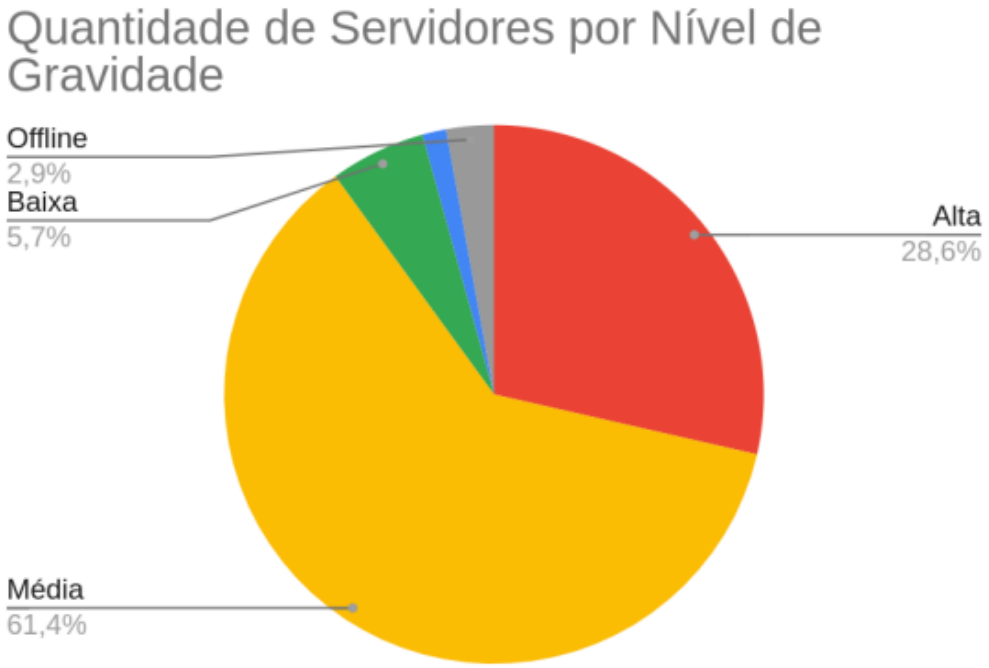
Considerando as novas diretrizes da Coordenação de Segurança da Informação da SETIC, a solicitação da equipe de Data Center da Coordenação de Infraestrutura da SETIC, realizou-se as análises nos seguintes hosts:

10.9.18.1	- 10.9.18.2	- 10.9.18.22	- 10.9.18.23	- 10.9.18.24 -
10.9.18.30	- 10.9.18.36	- 10.9.18.44	- 10.9.18.5	- 10.9.18.6 –
10.9.18.7	- 172.16.0.155	- 172.16.0.188	- 172.16.0.25	- 172.16.0.26 -
172.16.0.27	- 172.16.0.28	- 172.16.0.29	- 172.16.0.30	- 172.16.0.31 -
172.16.0.32	- 172.16.0.33	- 172.16.0.35	- 172.16.0.38	- 172.16.0.39 -
172.16.0.40	- 172.16.0.44	- 172.16.0.45	- 172.16.0.49	- 172.16.112.3 -
172.16.112.5	- 172.16.123.138	- 172.16.123.9	- 172.16.13.3	- 172.16.16.2 -
172.16.16.3	- 172.16.16.4	- 172.16.35.6	- 172.16.35.7	- 172.16.47.130
172.16.47.131	- 172.16.47.135	- 172.16.51.2	- 172.16.51.3	- 172.16.51.4 -
172.16.51.5	- 172.16.51.6	-172.16.6.133	- 172.16.6.134	- 172.16.6.136
172.16.6.142	- 172.16.6.143	- 172.16.6.144	- 172.16.6.15	- 172.16.6.151
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	- 172.16.6.169	- 172.16.6.2 -
172.16.6.20	- 172.16.6.21	- 172.16.6.3	-172.16.6.4	- 172.16.6.5

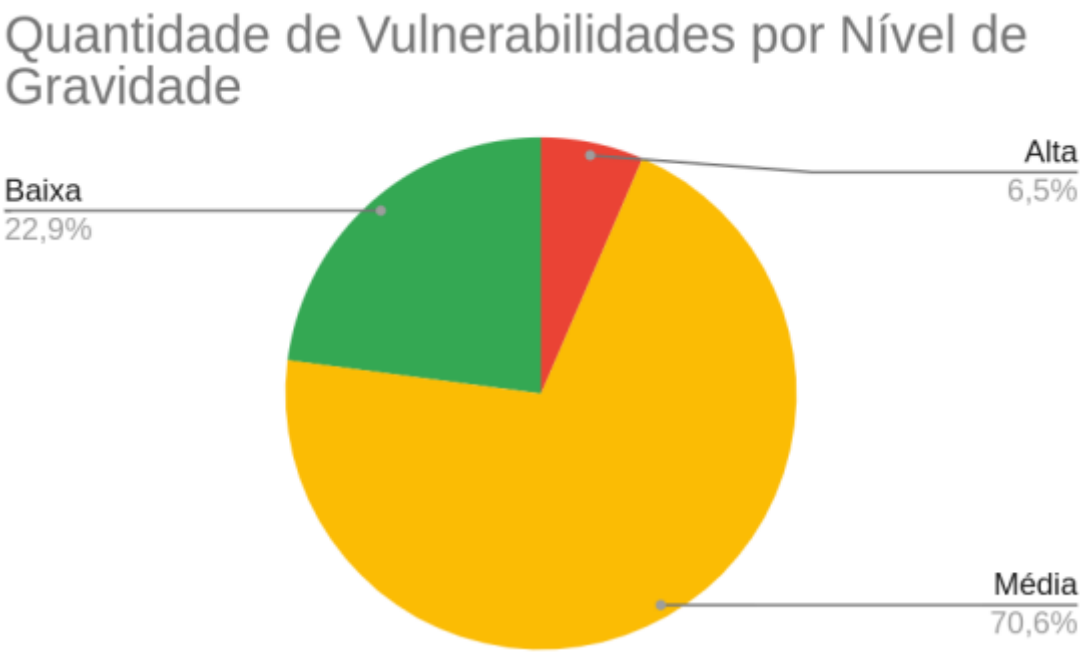
6 GRÁFICOS

Utilizando-se do OSSIM, considerando sua classificação das vulnerabilidades em 4 (quatro) diferentes níveis de gravidade (**crítico, alto, médio e baixo**) foi possível analisar **70** servidores de rede, dos quais **20 (28,6%)** apresentaram **alto** nível de gravidade, **43 (5,7%)** apresentaram **médio** nível, **4 (5,7%)** apresentaram **baixo** nível, conforme classificação do OSSIM,

destacando-se ainda que **1 (1,4%)** servidores não apresentaram **nenhuma** vulnerabilidade e **1 (1,4%)** endereços que não respondeu, ou desligados ou inalcançáveis., conforme gráfico abaixo:

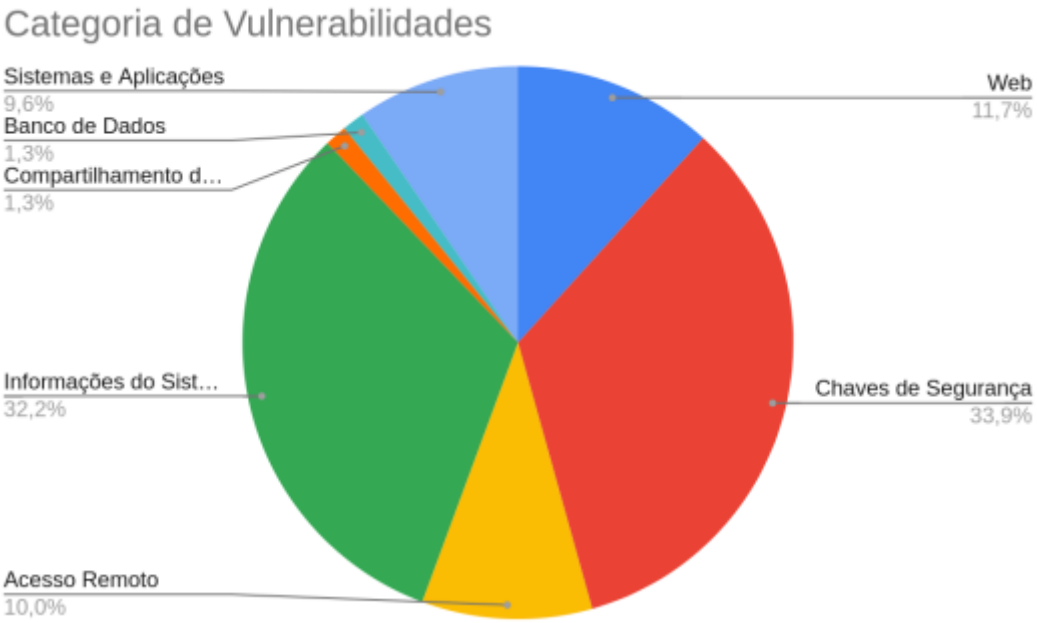


No que diz respeito às notificações apresentadas pelo OSSIM, destacam-se **554** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **36 (6,5%)** de **alto** nível, **391 (70,6%)** de **médio** nível e **127 (22,9%)** de **baixo** nível, conforme gráfico abaixo:



Além disso, com base nos relatórios do OSSIM, procurou-se categorizar as principais vulnerabilidades encontradas nos servidores de rede que foram analisados, criando as seguintes categorias: Web, Chaves de Segurança, Acesso Remoto, Informações do Sistema, Compartilhamento de Arquivos, Banco de Dados, 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 (27 servidores), Chaves de Segurança (78 servidores) e Informações do Sistema (74 servidores)**, conforme observado no gráfico abaixo:



7 AÇÕES CORRETIVAS

Após a realização das análises e produção dos relatórios, contendo informações do OSSIM, estes foram enviados ao setor de Datacenter, responsável por realizar as correções aplicando as medidas necessárias e/ou encaminhar ao responsável pelo servidor. Tal procedimento foi determinado pela Coordenação de Segurança da Informação da SETIC, considerando este o 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:

2022021013 - 2022021016 - 2022021027 - 2022021024 - 2022021017 - 2022021019
2022021021 - 2022021796 - 2022021792 - 2022021796 - 2022022013 - 2022022014
2022022016 - 2022022019 - 2022022028 - 2022022029 - 2022022031 - 2022022034
2022022035 - 2022022037 - 2022022038 - 2022022039 - 2022022041 - 2022022042
2022022044 - 2022020540 - 2022020541 - 2022020218 - 2022020216 - 2022020241
2022020242 - 2022020244 - 2022020530 - 2021122392 - 2021122393 - 2021122394
2022011364 - 2022011368 - 2022020086 - 2022020087 - 2022020090 - 2022020093
2022020095 - 2022020096 - 2022020098 - 2022020100 - 2022020101 - 2022020102
2022020105 - 2022020107 - 2022020109 - 2022020111 - 2022020112 - 2022020114
2022020115 - 2022020127 - 2022020128 - 2022020129 - 2022020130 - 2022020131
2022020132 - 2022020134 - 2022020135 - 2022020136 - 2022020137 - 2022020138
2022020139

Na sequência encontra-se uma tabela contendo informações sobre as referências, endereços de IP, datas das análises, 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.

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado (GLPI)	Data Chamado (GLPI)	sequencia chamado
172.16.16.2	10/02/2022	0	3	1	Média	DCE/RPC / SSL/TLS / TCP timestamps	-	2021122392		Resposta ao chamad
172.16.16.3	10/02/2022	0	3	1	Média	DCE/RPC / SSL/TLS / TCP timestamps	-	2021122393		Resposta ao chamad
172.16.16.4	07/02/2022	0	8	1	Média	DCE/RPC / SSL/TLS / TCP timestamps	-	2021122394		Resposta ao chamad

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)	sequencia chamado
172.16.35.6	17/02/2022	0	0	1	Baixa	ICMP Timestamp	infovia	2022011364	18-01-2022 11:00	Atendimento a cham
172.16.35.7	17/02/2022	0	3	1	Média	Missing `httpOnly` / S	infovia	2022011368	18-01-2022 11:02	Atendimento a cham
172.16.47.130	01/02/2022	0	4	2	Média	SSH / Cleartext Transr	-	2022020086	01-02-2022 10:50	Solicitação de correçã
172.16.47.131	01/02/2022	0	13	2	Média	DCE/RPC / SSL/TLS / T	calistemo.politec.local	2022020087	01-02-2022 10:53	Solicitação de correçã
172.16.47.135	01/02/2022	0	4	1	Média	DCE/RPC / SSL/TLS / T	amburana.politec.local	2022020090	01-02-2022 10:56	Solicitação de correçã
172.16.51.2	01/02/2022						-			
172.16.51.3	01/02/2022						-			
172.16.51.4	01/02/2022	0	3	0	Média	DCE/RPC / SSL/TLS		2022020093	01-02-2022 10:59	Solicitação de correçã
172.16.51.5	01/02/2022	0	11	1	Média	DCE/RPC / SSL/TLS / T	-	2022020095	01-02-2022 11:02	Solicitação de correçã
172.16.51.6	01/02/2022	0	3	1	Média	DCE/RPC / SSL/TLS / T		2022020096	01-02-2022 11:04	Solicitação de correçã

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado (GLPI)	Data Chamado (GLPI)	sequencia chamado
172.16.0.25	21/02/2022	0	4	0	Média	SSL/TLS / SSH	https://comuniquese.treina	2022021796	21-02-2022 09:14:32	Criação de registro

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado (GLPI)	Data Chamado (GLPI)	sequencia chamado
172.16.0.188	21/02/2022	0	10	2	Média	DCE/RPC / SSL/TLS / TCP timestamps	bolsaatleta.ro.gov.br - baba	2022021792	21-02-2022 09:07:05	Criação de registro

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado (GLPI)	Data Chamado (GLPI)	sequencia chamado
172.16.0.155	21/02/2022	0	5	0	Média	SSL/TLS / SSH	http://openshift.sistemas.r	2022021796	21-02-2022 09:14:32	Criação de registro

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)
10.9.18.1	07/02/2022	0	0	0				2022021013	14-02-2022 08:31
10.9.18.2	07/02/2022	1	2	2	Alta	OS End Of Life / Clea		2022021016	14-02-2022 08:35
10.9.18.22	07/02/2022	5	14	5	Alta	OS End Of Life / Free			
10.9.18.23	07/02/2022	4	14	5	Alta	OS End Of Life / Free			
10.9.18.24	07/02/2022	3	14	5	Alta	OS End Of Life / Free			
10.9.18.30	07/02/2022	5	13	5	Alta	OS End Of Life / Free			
10.9.18.36	07/02/2022	0	0	2	Baixa	TCP timestamps		2022021027	14-02-2022 08:48
10.9.18.44	07/02/2022	0	0	1	Baixa	ICMP Timestamp		2022021024	14-02-2022 08:45
10.9.18.5	07/02/2022	1	5	3	Alta	OS End Of Life / FTP		2022021017	14-02-2022 08:38
10.9.18.6	07/02/2022	0	4	2	Média	Cleartext Transmissi		2022021019	14-02-2022 08:40
10.9.18.7	07/02/2022	1	3	3	Alta	OS End Of Life / SSH		2022021021	14-02-2022 08:42

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)	sequencia chamado
172.16.6.133	01/02/2022	0	4	2	Média	SSH / HTTP Debuggin		2022020098	01-02-2022 11:07	Solicitação de correçã
172.16.6.134	01/02/2022	0	3	2	Média	WordPress / SSL/TLS /	http://ouropreto.sedam.ro.g	2022020100	01-02-2022 11:15	Solicitação de correçã
172.16.6.136	01/02/2022	0	7	2	Média	Mailserver / Cleartext		2022020101	01-02-2022 11:18	Solicitação de correçã
172.16.6.142	01/02/2022	1	16	2	Alta	HTTP.sys Remote Cod	-	2022020102	01-02-2022 11:22	Solicitação de correçã
172.16.6.143	01/02/2022	1	9	2	Alta	HTTP.sys Remote Cod	-	2022020105	01-02-2022 11:24	Solicitação de correçã
172.16.6.144	01/02/2022	1	11	2	Alta	HTTP.sys Remote Cod		2022020107	01-02-2022 11:27	Solicitação de correçã
172.16.6.15	01/02/2022	0	2	2	Média	Cleartext Transmissio		2022020109	01-02-2022 11:30	Solicitação de correçã
172.16.6.151	01/02/2022	1	8	2	Alta	MongoDB / Missing `h		2022020111	01-02-2022 11:33	Solicitação de correçã
172.16.6.152	01/02/2022	1	3	2	Alta	Tomcat / SSL/TLS / Cle	-	2022020112	01-02-2022 11:37	Solicitação de correçã
172.16.6.153	01/02/2022	0	1	2	Média	SSL/TLS / TCP timesta	-	2022020114	01-02-2022 11:39	Solicitação de correçã
172.16.6.155	01/02/2022	0	1	2	Média	SSL/TLS / TCP timesta	-	2022020115	01-02-2022 11:41	Solicitação de correçã
172.16.6.156	01/02/2022	1	1	2	Alta	SSH Brute Force / SSL	-	2022020127	01-02-2022 12:23	Solicitação de correçã
172.16.6.165	01/02/2022	0	1	2	Média	SSL/TLS / TCP timesta	-	2022020128	01-02-2022 12:26	Solicitação de correçã
172.16.6.166	01/02/2022	0	1	2	Média	SSL/TLS / TCP timesta	-	2022020129	01-02-2022 12:28	Solicitação de correçã
172.16.6.167	01/02/2022	1	3	2	Alta	Tomcat / SSL/TLS / Cle	-	2022020130	01-02-2022 12:30	Solicitação de correçã
172.16.6.168	01/02/2022	0	6	3	Média	SSH / SSL/TLS / Missir	-	2022020131	01-02-2022 12:32	Solicitação de correçã
172.16.6.169	01/02/2022	0	4	3	Média	SSH / SSL/TLS / TCP ti		2022020132	01-02-2022 12:34	Solicitação de correçã
172.16.6.2	01/02/2022	1	14	2	Alta	SMB Server / DCE/RP		2022020134	01-02-2022 12:37	Solicitação de correçã
172.16.6.20	01/02/2022	0	19	2	Média	DCE/RPC / SSL/TLS / T		2022020135	01-02-2022 12:39	Solicitação de correçã
172.16.6.21	01/02/2022	0	3	2	Média	WordPress / SSL/TLS /	-	2022020136	01-02-2022 12:41	Solicitação de correçã
172.16.6.3	01/02/2022	3	7	2	Alta	OS End Of Life / Webr		2022020137	01-02-2022 12:43	Solicitação de correçã
172.16.6.4	01/02/2022	0	11	2	Média	DCE/RPC / SSL/TLS / T		2022020138	01-02-2022 12:45	Solicitação de correçã
172.16.6.5	01/02/2022	1	15	2	Alta	SMB Server / DCE/RP		2022020139	01-02-2022 12:47	Solicitação de correçã

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)	sequencia chamado
172.16.0.26	21/02/2022	0	3	2	Média	SSL/TLS / SSH / TCP ti	-	2022022013	23-02-2022 08:28	Solicitação de correçã
172.16.0.27	21/02/2022	0	3	2	Média	SSL/TLS / SSH / TCP ti	-	2022022014	23-02-2022 08:30	Solicitação de correçã
172.16.0.28	21/02/2022	0	3	1	Média	SSL/TLS / SSH / ICMP	-	2022022016	23-02-2022 08:34	Solicitação de correçã
172.16.0.29	21/02/2022	0	3	0	Média	SSL/TLS / SSH	-	2022022019	23-02-2022 08:36	Solicitação de correçã
172.16.0.30	21/02/2022	0	3	0	Média	SSL/TLS / SSH	-	2022022028	23-02-2022 08:44	Solicitação de correçã
172.16.0.31	21/02/2022	0	1	2	Média	Cleartext Transmissio	proxy	2022022029	23-02-2022 08:47	Solicitação de correçã
172.16.0.32	21/02/2022	0	9	2	Média	DCE/RPC / SSL/TLS / T	-	2022022031	23-02-2022 08:55	Solicitação de correçã
172.16.0.33	21/02/2022	0	2	2	Média	SSH / TCP timestamps		2022022034	23-02-2022 09:17	Solicitação de correçã
172.16.0.35	21/02/2022	0	3	3	Média	SSH / TCP timestamps	-	2022022035	23-02-2022 09:19	Solicitação de correçã
172.16.0.38	21/02/2022	0	7	2	Média	Missing `httpOnly` / C		2022022037	23-02-2022 09:22	Solicitação de correçã
172.16.0.39	21/02/2022	0	0	2	Baixa	TCP timestamps		2022022038	23-02-2022 09:24	Solicitação de correçã
172.16.0.40	21/02/2022	0	4	0	Média	DCE/RPC / SQL Server	-	2022022039	23-02-2022 09:26	Solicitação de correçã
172.16.0.44	21/02/2022	1	12	2	Alta	SMB Server / DCE/RP	fedegoso.rondonia.local	2022022041	23-02-2022 09:28	Solicitação de correçã
172.16.0.45	21/02/2022	0	13	1	Média	DCE/RPC / ICMP Time		2022022042	23-02-2022 09:30	Solicitação de correçã
172.16.0.49	21/02/2022	0	2	2	Média	SSH / TCP timestamps	-	2022022044	23-02-2022 09:32	Solicitação de correçã

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)	sequencia chamado
172.16.112.3	07/02/2022	0	2	2	Média	SSH / TCP timestamps	-	2022020540	08-02-2022 09:04	Solicitação de correçã
172.16.112.5	07/02/2022	1	5	2	Alta	Redis Server / SSH / S	-	2022020541	08-02-2022 09:06	Solicitação de correçã
172.16.123.138	02/02/2022	0	11	2	Média	FTP / Cleartext Transn	https://api-dev-carteiravisita	2022020218 - 20	02-02-2022 10:30:44	Atendimento a chama
172.16.123.9	2/2/2022	0	7	2	Média	SSL/TLS / Missing `htt	portainer-prod.sejus.ro.gov.	2022020241 - 20	02-02-2022 11:51:44	Atendimento a chama
172.16.13.3	07/02/2022	2	5	1	Alta	HP Data Protector Bac		2022020530	08-02-2022 08:31	Solicitação de correçã

8 REFERÊNCIAS

BRASIL. Instrução normativa Nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. Diário Oficial da República Federativa do Brasil. Brasília, 28 maio 2020. Seção 1, p. 13.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação. Rio de Janeiro: 2013.

SETIC/Governo de Rondônia. Política de Segurança da Informação (2021) - finalidade de assegurar a segurança das informações trafegadas na rede de dados da Superintendência Estadual de Tecnologia da Informação - SETIC, regulando a proteção dos dados, informações e conhecimentos.