SETIC
Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

RELATÓRIO MARÇO/2022
COSEGI

2022

Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

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).

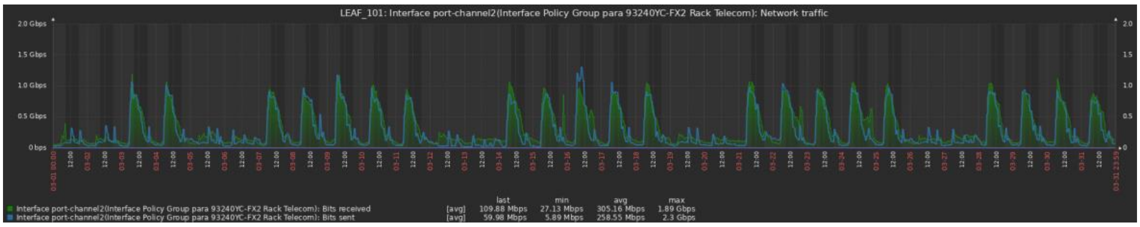
SUMÁRIO

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 março.

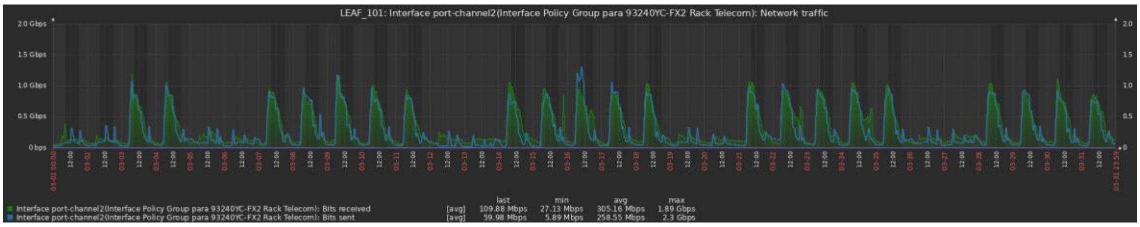
2 TRÁFEGO DE REDE

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

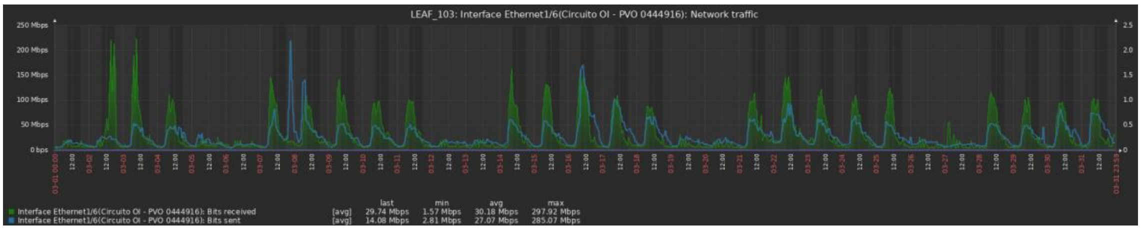


Monitoramento de tráfego Cores SETIC

Além disso, foram consumidos **42 TB** de tráfego da Internet, considerando acesso dos usuários a aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.

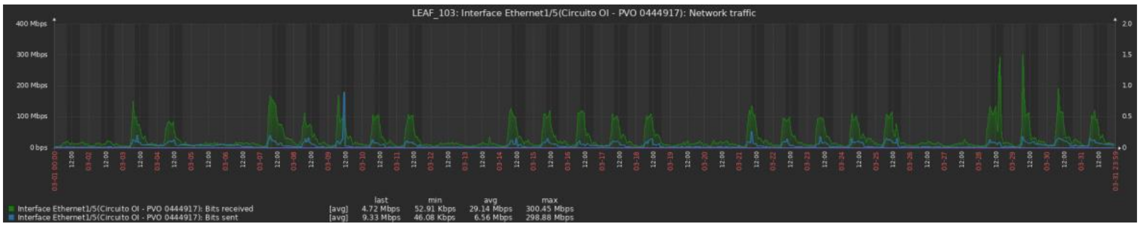


Monitoramento de tráfego Cores Link Telebrás



Monitoramento de tráfego Cores Link Oi – SETIC

* O link da operadora OI é utilizado para maioria dos serviços críticos publicados pela DETIC (SEI, E-mail, Portais Governo RO...)



Monitoramento de tráfego Cores Link Oi - INFOVIA

2.1 Consumo por Secretaria

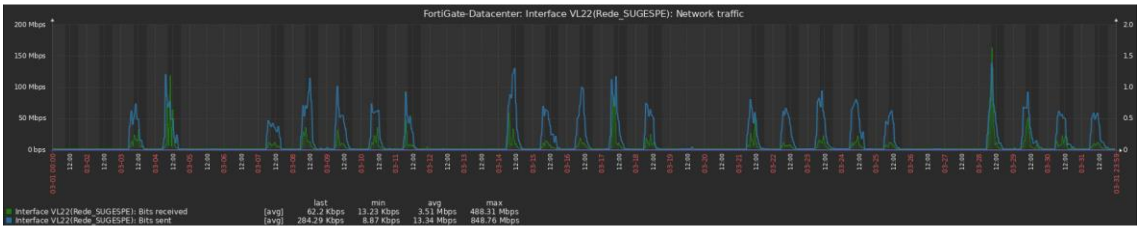
Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **13 TB** de informação trafegada no mês deste relatório por secretaria.

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

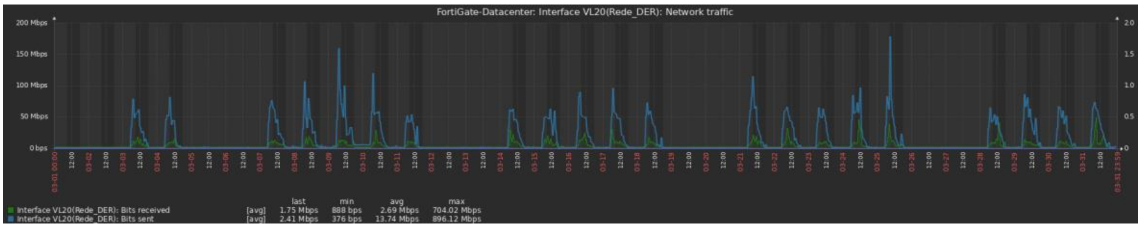
Secretária SUGESP: **5 TB**

Secretária DER/SEOSP: **5 TB**

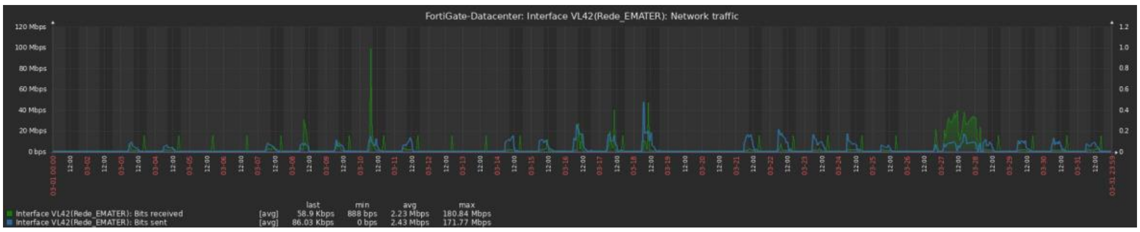
Secretária EMATER: **3 TB**



Monitoramento de tráfego SUGESP



Monitoramento de tráfego DER/SEOSP

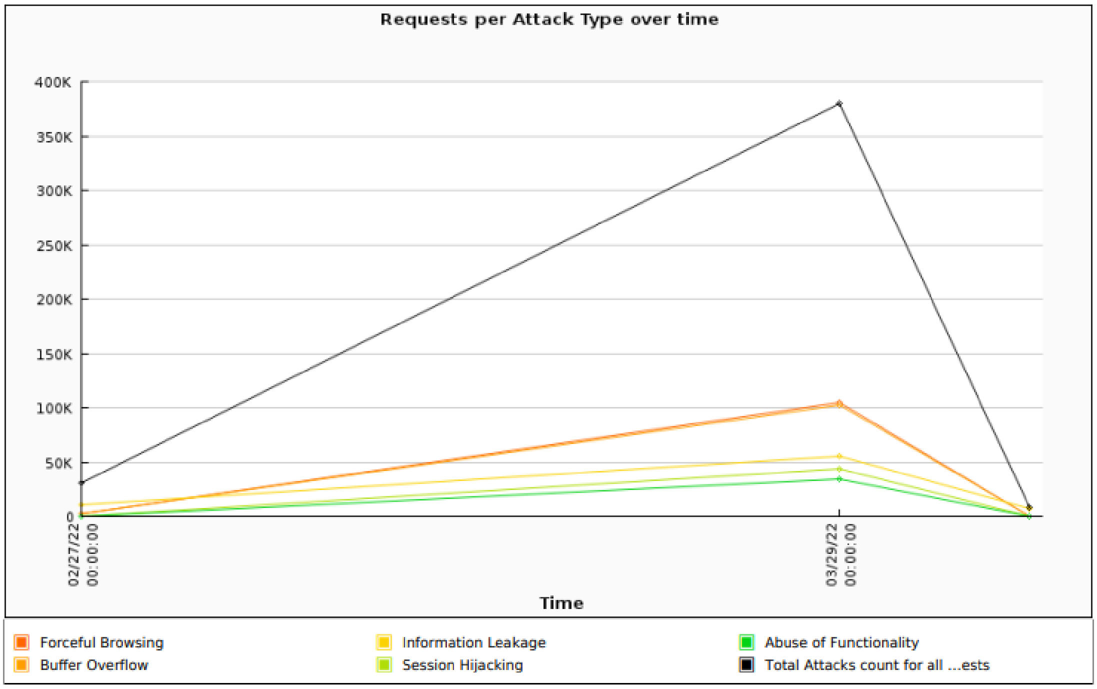


Monitoramento de tráfego EMATER

3 ATAQUES

Durante o mês de **Março** as tentativas de ataques bloqueados através do firewall de aplicação Web (WAF), no qual protege contra ameaças emergentes, foi no total de **364.229** (Trezentos e sessenta e quatro mil, duzentos e vinte e nove) de tentativas de ataques. E segue os top 5 tentativas de ataque:

1	Forceful Browsing: 107.462
2	Buffer Overflow: 105.095
3	Information Leakage: 73.719
4	Session Hijacking: 42.990
5	Abuse of Functionality: 34.963



Attack Type	▼ Requests
Forceful Browsing	107462
Buffer Overflow	105095
Information Leakage	73719
Session Hijacking	42990
Abuse of Functionality	34963
Total Attacks count for all requests	419807

Displaying **5** out of total **23** entries

Também foram bloqueadas um total de **429.683** (Quatrocentos e vinte e nove mil, seiscentos e oitenta e três) 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].

[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.

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 **87** servidores de rede, dos quais **2 (2,3%)** apresentaram **alto** nível de gravidade, **76 (87,4%)** apresentaram **médio** nível, **2 (2,3%)** apresentaram **baixo** nível, conforme classificação do OSSIM, destacando-se ainda que **nenhum** servidores não apresentaram **nenhuma** vulnerabilidade.

Também encontramos **27 (8,0%)** 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 OSSIM detectou **505** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **3 (0,6%)** de **alto** nível, **382 (75,6%)** de **médio** nível e **120 (23,8%)** de **baixo** nível.

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

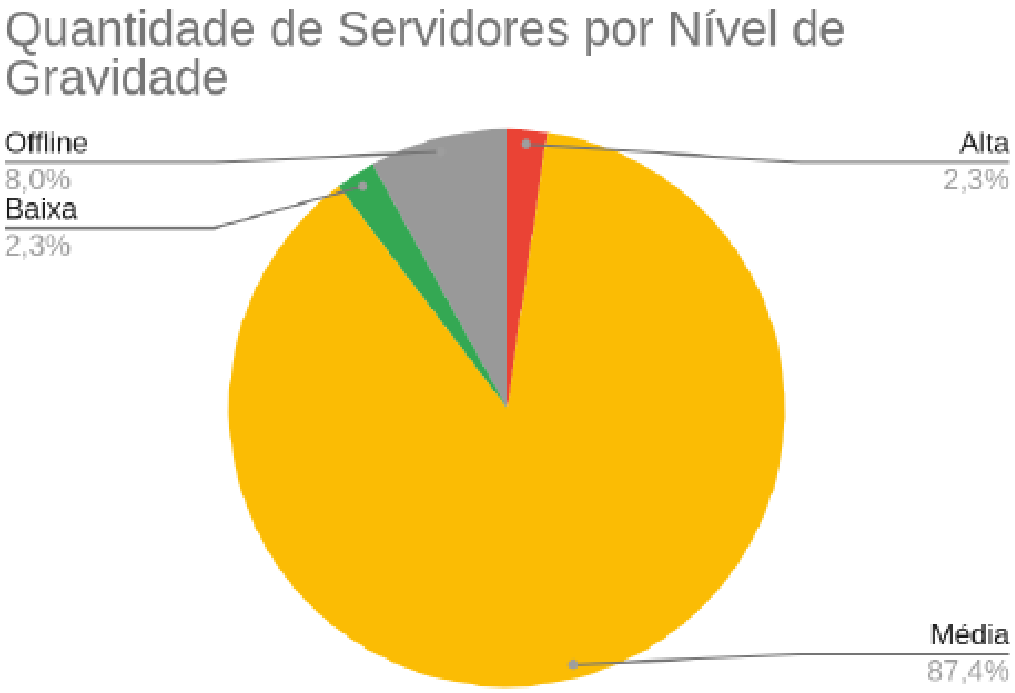
5 CONTEXTO DA ANÁLISE DE VULNERABILIDADE

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:

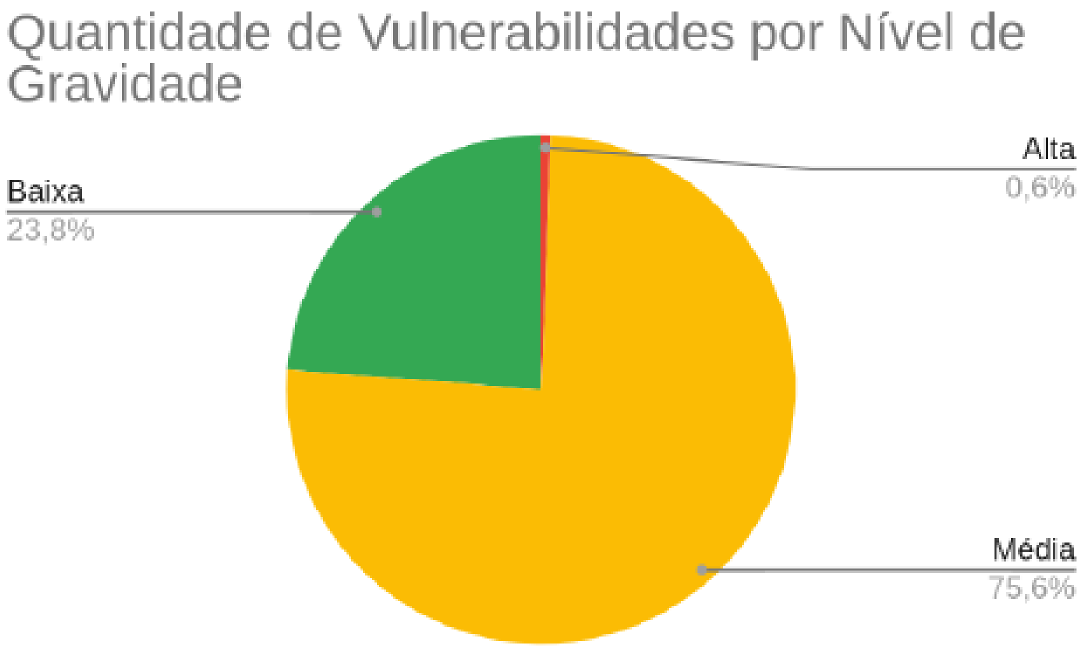
172.16.0.57	- 172.16.0.64	- 172.16.0.66	- 172.16.0.69	- 172.16.0.71
172.16.0.73	- 172.16.0.74	- 172.16.0.75	- 172.16.0.78	- 172.16.0.80
172.16.0.82	- 172.16.0.84	- 172.16.0.85	- 172.16.0.86	- 172.16.0.87
172.16.0.89	- 172.16.0.90	- 172.16.0.92	- 172.16.0.97	- 172.16.0.98
172.16.1.100	- 172.16.1.102	- 172.16.1.103	- 172.16.1.104	- 172.16.1.105
172.16.1.107	- 172.16.1.112	- 172.16.1.123	- 172.16.1.127	- 172.16.1.128
172.16.1.129	- 172.16.1.13	- 172.16.1.130	- 172.16.1.131	- 172.16.1.135
172.16.1.136	- 172.16.1.137	- 172.16.1.139	- 172.16.1.14	- 172.16.1.140
172.16.1.141	- 172.16.1.142	- 172.16.1.143	- 172.16.1.144	- 172.16.1.145
172.16.1.147	- 172.16.1.15	- 172.16.1.16	- 172.16.1.17	- 172.16.1.18
172.16.1.182	- 172.16.1.19	- 172.16.1.190	- 172.16.1.192	- 172.16.1.202
172.16.1.203	- 172.16.1.204	- 172.16.1.205	- 172.16.1.209	- 172.16.1.234
172.16.1.236	- 172.16.1.24	- 172.16.1.25	- 72.16.1.28	- 172.16.1.30
172.16.1.31	- 172.16.1.33	- 172.16.1.36	- 172.16.1.37	- 172.16.1.43
172.16.1.44	- 172.16.1.45	- 172.16.1.46	- 172.16.1.51	- 172.16.1.52
172.16.1.53	- 172.16.1.55	- 172.16.1.57	- 172.16.1.61	- 172.16.1.62
172.16.1.63	- 172.16.1.64	- 172.16.1.65	- 172.16.1.66	- 172.16.1.69
172.16.1.80	- 172.16.1.94.			

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 **87** servidores de rede, dos quais **2 (2,3%)** apresentaram **alto** nível de gravidade, **76 (87,4%)** apresentaram **médio** nível, **2 (2,3%)** apresentaram **baixo** nível, conforme classificação do OSSIM, destacando-se ainda que **nenhum** servidor não apresentaram **nenhuma** vulnerabilidade. Também encontramos **7 (8,0%)** endereços que não responderam, ou desligados ou inalcançáveis, conforme gráfico abaixo:

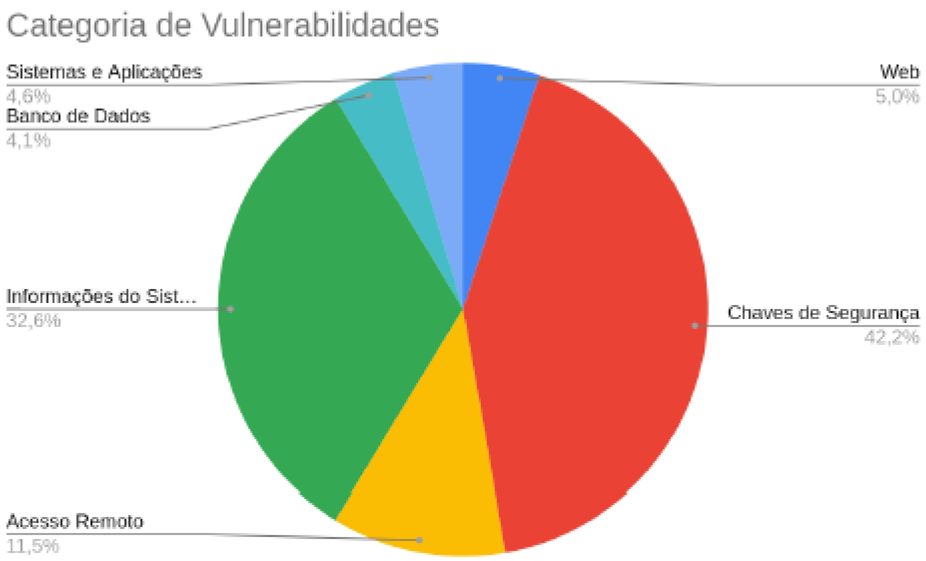


No que diz respeito às notificações apresentadas pelo OSSIM, destacam-se **505** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **3 (0,6%)** de **alto** nível, **382 (75,6%)** de **médio** nível e **120 (23,8%)** de **baixo** nível, 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 (11 servidores), Chaves de Segurança (92 servidores) e Informações do Sistema (71 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:

2022030678 - 2022030682 - 2022030686 - 2022030689 - 2022030690 - 2022030692 - 2022030694 - 2022030701 - 2022030702 - 2022030706 - 2022030707 - 2022030708 - 2022030709 - 2022030710 - 2022030713 - 2022030714 - 2022030715 - 2022030716 - 2022030718 - 2022030719 - 2022030721 - 2022030724 - 2022030727 - 2022030728 - 2022030729 - 2022030732 - 2022030734 - 2022030736 - 2022030739 - 2022030744 - 2022030748 - 2022031019 - 2022031021 - 2022031039 - 2022031041 - 2022031043 - 2022031351 - 2022031353 - 2022031356 - 2022031361 - 2022031362 - 2022031365 - 2022031377 - 2022031378 - 2022031379 - 2022031382 - 2022031383 - 2022031384 - 2022031386 - 2022031388 - 2022031391 - 2022031393 - 2022031396 - 2022031398 - 2022031399 - 2022031404 - 2022031405 - 2022031408 - 2022031409 - 2022031422 - 2022031426 - 2022031428 - 2022031434 - 2022031437 - 2022031439 - 2022031440 - 2022031443 - 2022031444 - 2022031445 - 2022031449 - 2022031450 - 2022031452 - 2022031454 - 2022031455 - 2022031456 - 2022031457 - 2022031458 - 2022031460 - 2022031461 - 2022031463.

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	Data Chamado (GLPI)	sequencia chamado
172.16.0.57	07/03/2022	0	2	2	Média	SSH / TCP timestamps		2022030678	10-03-2022 08:17	Solicitação de correç
172.16.0.64	07/03/2022	0	0	2	Baixa	TCP timestamps		2022030682	10-03-2022 08:24	Solicitação de correç
172.16.0.66	07/03/2022	0	2	2	Média	SSH / TCP timestamps	-	2022030686	10-03-2022 08:29	Solicitação de correç
172.16.0.69	07/03/2022	0	5	1	Média	DCE/RPC / SSL/TLS / T	-	2022030689	10-03-2022 08:33	Solicitação de correç
172.16.0.71	07/03/2022	0	2	2	Média	SSH / TCP timestamps		2022030690	10-03-2022 08:36	Solicitação de correç
172.16.0.73	07/03/2022	0	4	1	Média	DCE/RPC / SSL/TLS / T	cajueiro.rondonia.local	2022030692	10-03-2022 08:39	Solicitação de correç
172.16.0.74	07/03/2022	0	4	1	Média	DCE/RPC / SSL/TLS / T	piuna.rondonia.local	2022030694	10-03-2022 08:42	Solicitação de correç
172.16.0.75	07/03/2022					off	http://172.16.0.75/			
172.16.0.78	07/03/2022	0	3	2	Média	HTTP / SSH / TCP time		2022030701	10-03-2022 09:04	Solicitação de correç
172.16.0.80	07/03/2022	0	3	1	Média	DCE/RPC / SSL/TLS / T	amoreira	2022030702	10-03-2022 09:08	Solicitação de correç
172.16.0.82	07/03/2022	0	2	2	Média	SSH / TCP timestamps	-	2022030706	10-03-2022 09:18	Solicitação de correç
172.16.0.84	07/03/2022	0	13	1	Média	DCE/RPC / SQL Server		2022030707	10-03-2022 09:21	Solicitação de correç
172.16.0.85	07/03/2022	0	4	0	Média	DCE/RPC / SQL Server		2022030708	10-03-2022 09:24	Solicitação de correç
172.16.0.86	07/03/2022	0	4	0	Média	DCE/RPC / SQL Server		2022030709	10-03-2022 09:26	Solicitação de correç
172.16.0.87	07/03/2022	0	2	1	Média	DCE/RPC / SSL/TLS / T		2022030710	10-03-2022 09:29	Solicitação de correç
172.16.0.89	07/03/2022	0	5	0	Média	DCE/RPC / SQL Server		2022030713	10-03-2022 09:31	Solicitação de correç
172.16.0.90	07/03/2022	0	6	2	Média	FTP Unencrypted / M		2022030714	10-03-2022 09:34	Solicitação de correç
172.16.0.92	07/03/2022					off				
172.16.0.97	07/03/2022	0	12	1	Média	DCE/RPC / SSL/TLS / I		2022030715	10-03-2022 09:36	Solicitação de correç
172.16.0.98	07/03/2022	0	2	2	Média	SSH / TCP timestamps	oiti.rondonia.local	2022030716	10-03-2022 09:40	Solicitação de correç
172.16.1.100	09/03/2022	0	3	2	Média	SSH / TCP timestamps	GABIROBA	2022030718	10-03-2022 09:43	Solicitação de correç
172.16.1.102	09/03/2022	2	16	3	Alta	MortBay Eclipse Jetty	-	2022030719	10-03-2022 09:46	Solicitação de correç
172.16.1.103	09/03/2022	0	3	3	Média	SSH / TCP timestamps	CEBOLAO	2022030721	10-03-2022 09:53	Solicitação de correç
172.16.1.104	09/03/2022	0	4	2	Média	Cleartext Transmissio	-	2022030724	10-03-2022 09:58	Solicitação de correç
172.16.1.105	09/03/2022	0	2	1	Média	DCE/RPC / TCP timest	anaxagorea.rondonia.local	2022030727	10-03-2022 10:02	Solicitação de correç
172.16.1.107	09/03/2022	0	3	1	Média	HTTP / SSH / ICMP tin	LEITEIRO	2022030728	10-03-2022 10:05	Solicitação de correç

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)	sequencia chamado
172.16.1.112	09/03/2022	0	6	2	Média	DCE/RPC / SSL/TLS / T	-	2022030729	10-03-2022 10:08	Solicitação de correç
172.16.1.123	09/03/2022	0	2	2	Média	SSH / TCP timestamps	RUDGEA	2022030732	10-03-2022 10:14	Solicitação de correç
172.16.1.127	09/03/2022	0	11	1	Média	DCE/RPC / SSL/TLS / I		2022030734	10-03-2022 10:17	Solicitação de correç
172.16.1.128	09/03/2022	0	3	2	Média	FTP / SSH / TCP times		2022030736	10-03-2022 10:19	Solicitação de correç
172.16.1.129	09/03/2022	0	3	2	Média	SSH / Cleartext Transr		2022030739	10-03-2022 10:21	Solicitação de correç
172.16.1.13	09/03/2022	0	1	0	Média	SSL/TLS	-	2022030744	10-03-2022 10:24	Solicitação de correç
172.16.1.130	09/03/2022	0	2	1	Média	SSH / ICMP Timestam	TIMBURI - http://treinamen	2022030748	10-03-2022 10:26	Solicitação de correç
172.16.1.131	10/03/2022	0	3	2	Média	HTTP Debugging Metl	PINDAIVA - http://dev.sei.si	2022031019	14-03-2022 10:25	Solicitação de correç
172.16.1.135	10/03/2022	0	2	2	Média	SSH / TCP timestamps	BOLEIRO	2022031021	14-03-2022 10:33	Solicitação de correç
172.16.1.136	10/03/2022	0	5	1	Média	HTTP / Source Contro	patadevaca - http://172.16.1	2022031039	14-03-2022 11:23	Solicitação de correç
172.16.1.137	10/03/2022	1	2	0	Alta	PostgreSQL / SSH	LIQUIDAMBA	2022031041	14-03-2022 11:29	Solicitação de correç
172.16.1.139	10/03/2022	0	2	2	Média	SSH / TCP timestamps	PAUFORMIGA	2022031043	14-03-2022 11:32	Solicitação de correç
172.16.1.14	10/03/2022	0	4	1	Média	SSL/TLS / SSH / ICMP	https://sei.sistemas.ro.gov.b	2022031351	16-03-2022 08:17	Solicitação de correç
172.16.1.140	10/03/2022	0	15	4	Média	SSL/TLS / Grafana / SS		2022031353	16-03-2022 08:21	Solicitação de correç
172.16.1.141	10/03/2022	0	15	4	Média	SSL/TLS / Grafana / SS		2022031356	16-03-2022 08:29	Solicitação de correç
172.16.1.142	10/03/2022	0	15	4	Média	SSL/TLS / Grafana / SS		2022031361	16-03-2022 08:34	Solicitação de correç
172.16.1.143	10/03/2022	0	15	4	Média	SSL/TLS / Grafana / SS		2022031362	16-03-2022 08:35	Solicitação de correç
172.16.1.144	10/03/2022	0	15	4	Média	SSL/TLS / Grafana / SS		2022031365	16-03-2022 08:37	Solicitação de correç
172.16.1.145	10/03/2022	0	15	4	Média	SSL/TLS / Grafana / SS		2022031377	16-03-2022 09:12	Solicitação de correç
172.16.1.147	10/03/2022	0	0	2	Baixa	TCP timestamps		2022031378	16-03-2022 09:14	Solicitação de correç
172.16.1.15	10/03/2022	0	1	2	Média	Cleartext Transmissio		2022031379	16-03-2022 09:16	Solicitação de correç
172.16.1.16	10/03/2022	0	13	1	Média	DCE/RPC / SQL Server		2022031382	16-03-2022 09:20	Solicitação de correç
172.16.1.17	10/03/2022	0	10	2	Média	DCE/RPC / SSL/TLS / I		2022031383	16-03-2022 09:22	Solicitação de correç
172.16.1.18	10/03/2022	0	10	2	Média	DCE/RPC / SSL/TLS / I		2022031384	16-03-2022 09:24	Solicitação de correç
172.16.1.182	10/03/2022	0	1	0	Média	SSL/TLS		2022031386	16-03-2022 09:26	Solicitação de correç
172.16.1.19	10/03/2022	0	2	1	Média	SSH / TCP timestamps	-	2022031388	16-03-2022 09:29	Solicitação de correç
172.16.1.190	10/03/2022	0	2	2	Média	SSH / TCP timestamps	sumauma	2022031391	16-03-2022 09:31	Solicitação de correç
172.16.1.192	10/03/2022					off				
172.16.1.202	10/03/2022	0	5	1	Média	Mailserver / SSL/TLS /	LOUVEIRA - http://treiname	2022031393	16-03-2022 09:34	Solicitação de correç
172.16.1.203	10/03/2022	0	2	1	Média	SSH / ICMP Timestam	JARACATIA	2022031396	16-03-2022 09:38	Solicitação de correç
172.16.1.204	10/03/2022	0	2	1	Média	SSH / ICMP Timestam	ESCUMILHA - http://treinam	2022031398	16-03-2022 09:44	Solicitação de correç
172.16.1.205	10/03/2022	0	2	0	Média	SSH	CAJUACU	2022031399	16-03-2022 09:49	Solicitação de correç
172.16.1.209	10/03/2022	0	2	2	Média	SSH / TCP timestamps	LEUCENA	2022031404	16-03-2022 09:55	Solicitação de correç
172.16.1.234	10/03/2022					off	CUPANIA			
172.16.1.236	10/03/2022					off				
172.16.1.24	10/03/2022	0	9	2	Média	DCE/RPC / SSL/TLS / I	-	2022031405	16-03-2022 09:58	Solicitação de correç
172.16.1.25	10/03/2022	0	2	2	Média	SSH / TCP timestamps	AZEVINHO	2022031408	16-03-2022 10:02	Solicitação de correç
172.16.1.28	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031409	16-03-2022 10:04	Solicitação de correç
172.16.1.30	10/03/2022	0	13	1	Média	SSL/TLS / DCE/RPC / I	-	2022031422	16-03-2022 10:44	Solicitação de correç

IP	Data da Análise	Alta	Média	Baixa	Principal Gravidade	Principais Falhas	Endereço Externo/Interno	Num. Chamado	Data Chamado (GLPI)	sequencia chamado
172.16.1.31	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031426	16-03-2022 10:46	Solicitação de correç
172.16.1.33	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031428	16-03-2022 10:51	Solicitação de correç
172.16.1.36	10/03/2022						-			
172.16.1.37	10/03/2022	0	2	1	Média	SSH / ICMP Timestam	REPODATA-SEI	2022031434	16-03-2022 11:06	Solicitação de correç
172.16.1.43	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031437	16-03-2022 11:09	Solicitação de correç
172.16.1.44	10/03/2022	0	2	0	Média	SSH	-	2022031439	16-03-2022 11:12	Solicitação de correç
172.16.1.45	10/03/2022	0	2	0	Média	SSH	-	2022031440	16-03-2022 11:14	Solicitação de correç
172.16.1.46	10/03/2022	0	2	2	Média	SSH / TCP timestamps	candeia	2022031443	16-03-2022 11:16	Solicitação de correç
172.16.1.51	10/03/2022	0	3	1	Média	HTTP Debugging Metl	BUTIA - http://sei.sistemas.r	2022031444	16-03-2022 11:21	Solicitação de correç
172.16.1.52	10/03/2022	0	3	1	Média	HTTP Debugging Metl	CEIBA - http://sei.sistemas.r	2022031445	16-03-2022 11:23	Solicitação de correç
172.16.1.53	10/03/2022	0	3	1	Média	HTTP Debugging Metl	DENDEZEIRO - http://sei.sist	2022031449	16-03-2022 11:29	Solicitação de correç
172.16.1.55	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031450	16-03-2022 11:31	Solicitação de correç
172.16.1.57	10/03/2022	0	5	0	Média	DCE/RPC / SQL Server		2022031452	16-03-2022 11:36	Solicitação de correç
172.16.1.61	10/03/2022	0	13	1	Média	DCE/RPC / SQL Server		2022031454	16-03-2022 11:38	Solicitação de correç
172.16.1.62	10/03/2022	0	3	0	Média	SSL/TLS / SSH		2022031455	16-03-2022 11:40	Solicitação de correç
172.16.1.63	10/03/2022	0	3	0	Média	SSL/TLS / SSH		2022031456	16-03-2022 11:42	Solicitação de correç
172.16.1.64	10/03/2022	0	3	0	Média	SSL/TLS / SSH		2022031457	16-03-2022 11:43	Solicitação de correç
172.16.1.65	10/03/2022	0	3	0	Média	SSL/TLS / SSH		2022031458	16-03-2022 11:45	Solicitação de correç
172.16.1.66	10/03/2022	0	3	0	Média	SSL/TLS / SSH		2022031460	16-03-2022 11:47	Solicitação de correç
172.16.1.69	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031461	16-03-2022 11:49	Solicitação de correç
172.16.1.80	10/03/2022	0	2	2	Média	SSH / TCP timestamps		2022031463	16-03-2022 11:51	Solicitação de correç
172.16.1.94	10/03/2022									

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.