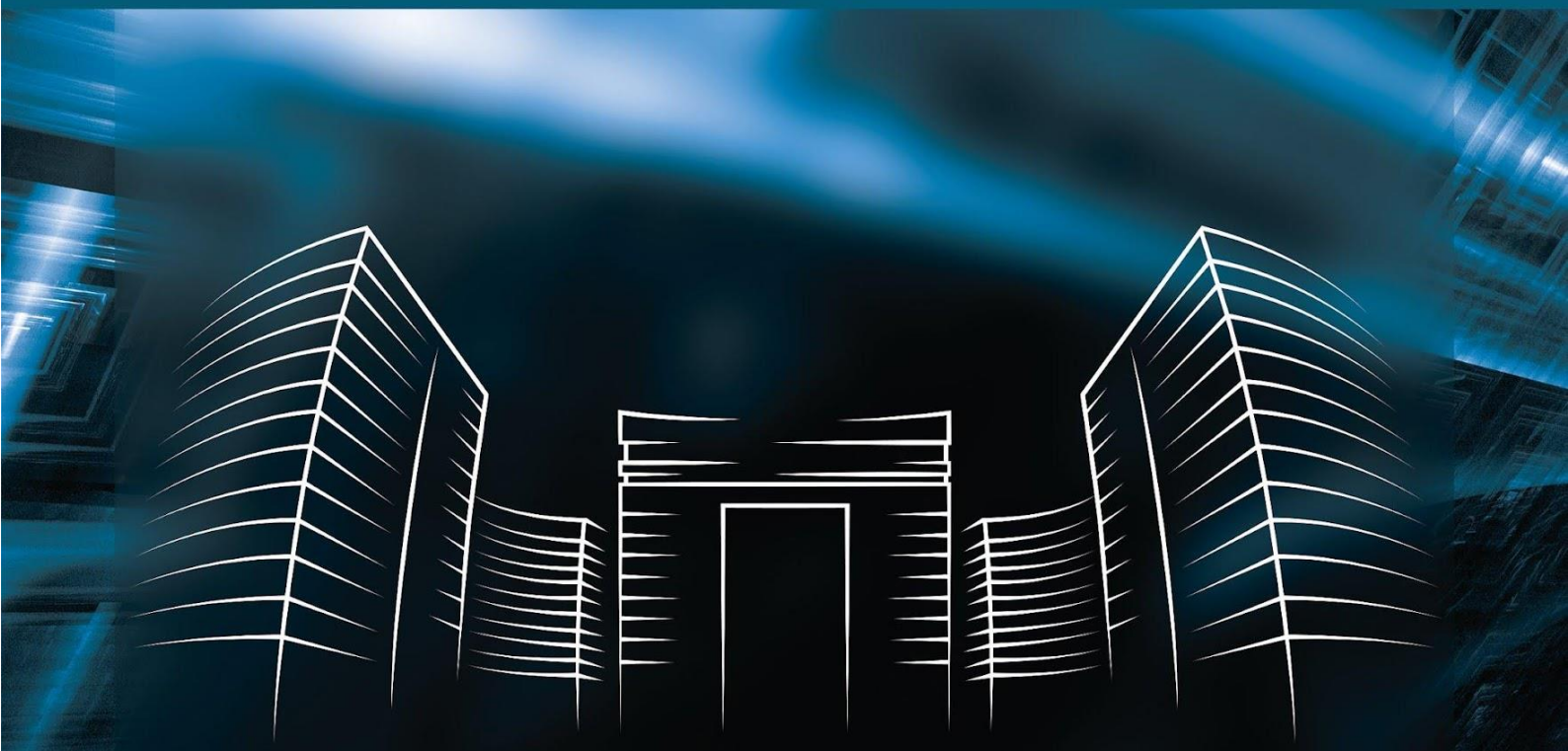
SETIC
Superintendência Estadual de
Tecnologia da Informação e
Comunicação

Governo do Estado de
RONDÔNIA

RELATÓRIO JANEIRO/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	07/02/2022	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).

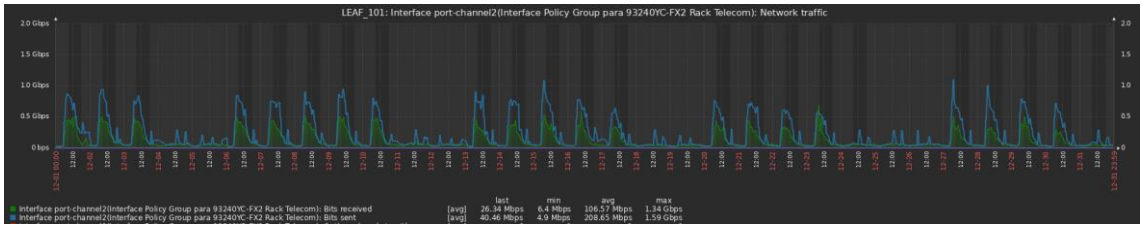
SUMÁRIO

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 Janeiro.

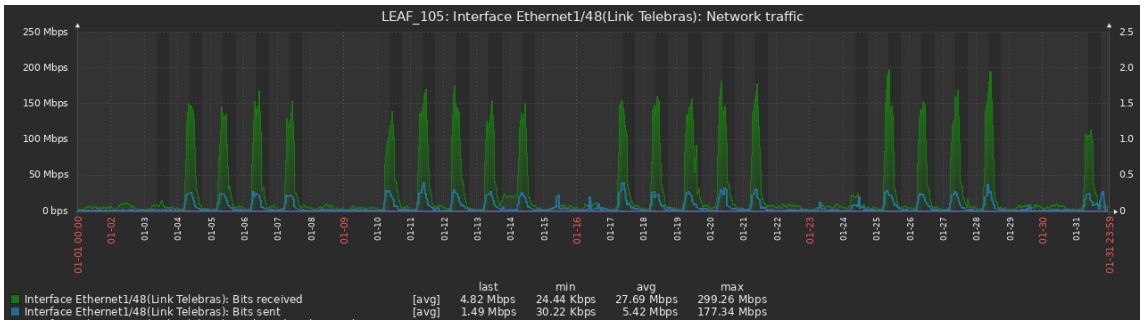
2 TRÁFEGO DE REDE

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

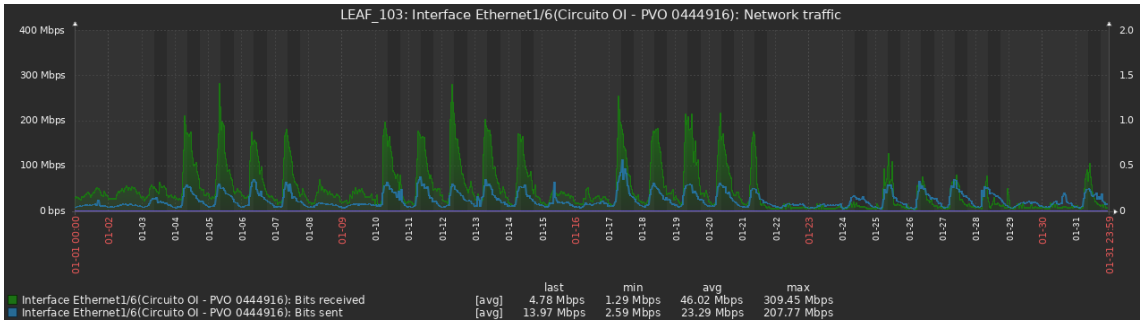


Monitoramento de tráfego Cores SETIC

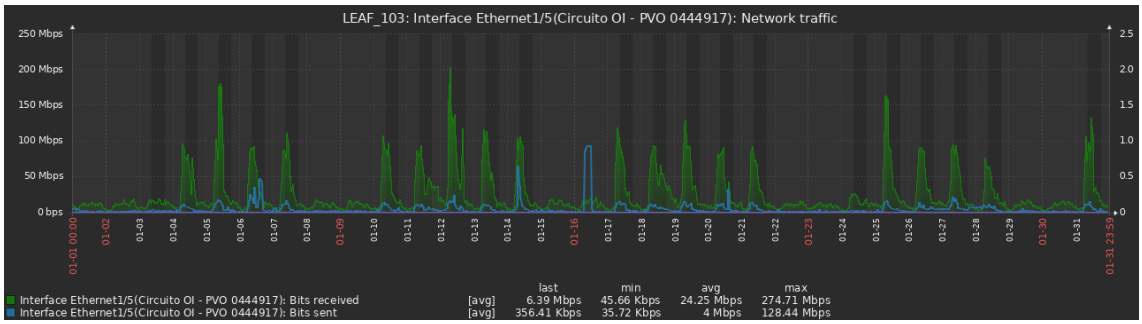
Além disso, foram consumidos **43 TB** de tráfego da Internet, considerando acesso dos usuários a aplicações de Governo expostas na Internet e acesso a serviços pelo público geral.



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

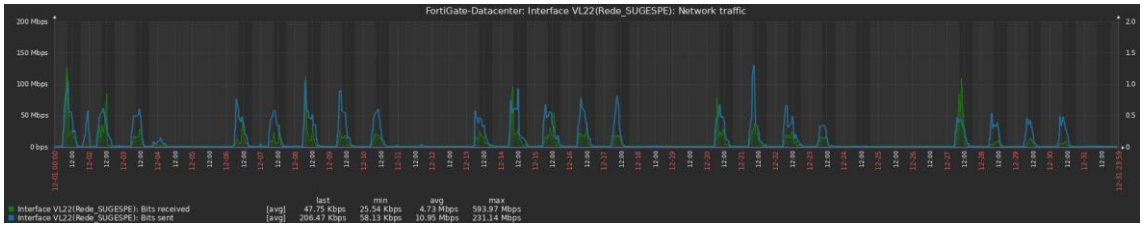
Considerando os dados de tráfego de rede transferidos via Cores de Comunicação de Dados da SETIC, entre estações de trabalho do Palácio Rio Madeira, INFOVIA e serviços hospedados, aferimos o Volume Total de **12 TB** de informação trafegada no mês deste relatório por secretaria.

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

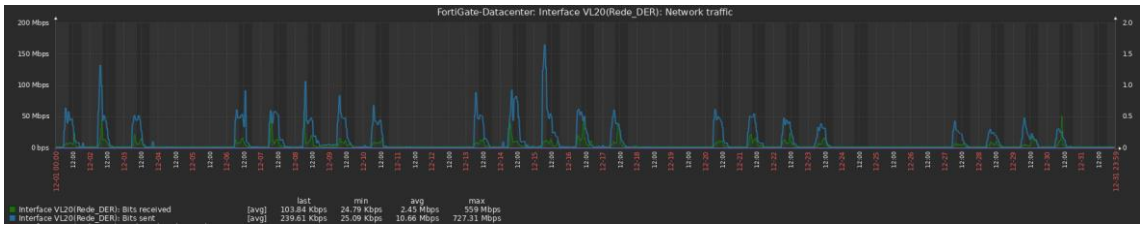
Secretária SUGESP: **4 TB**

Secretária DER/SEOSP: **3 TB**

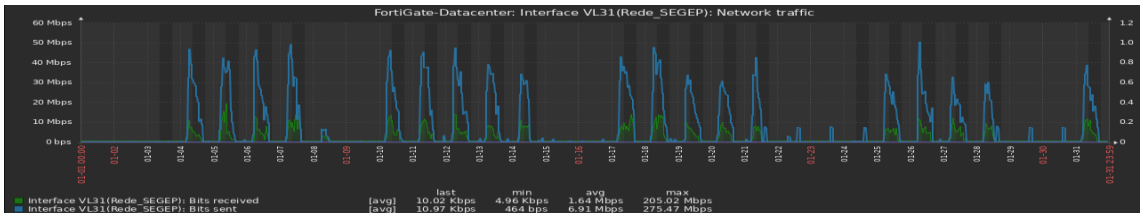
Secretária SEGEP: **2 TB**



Monitoramento de tráfego SUGESP



Monitoramento de tráfego DER/SEOSP

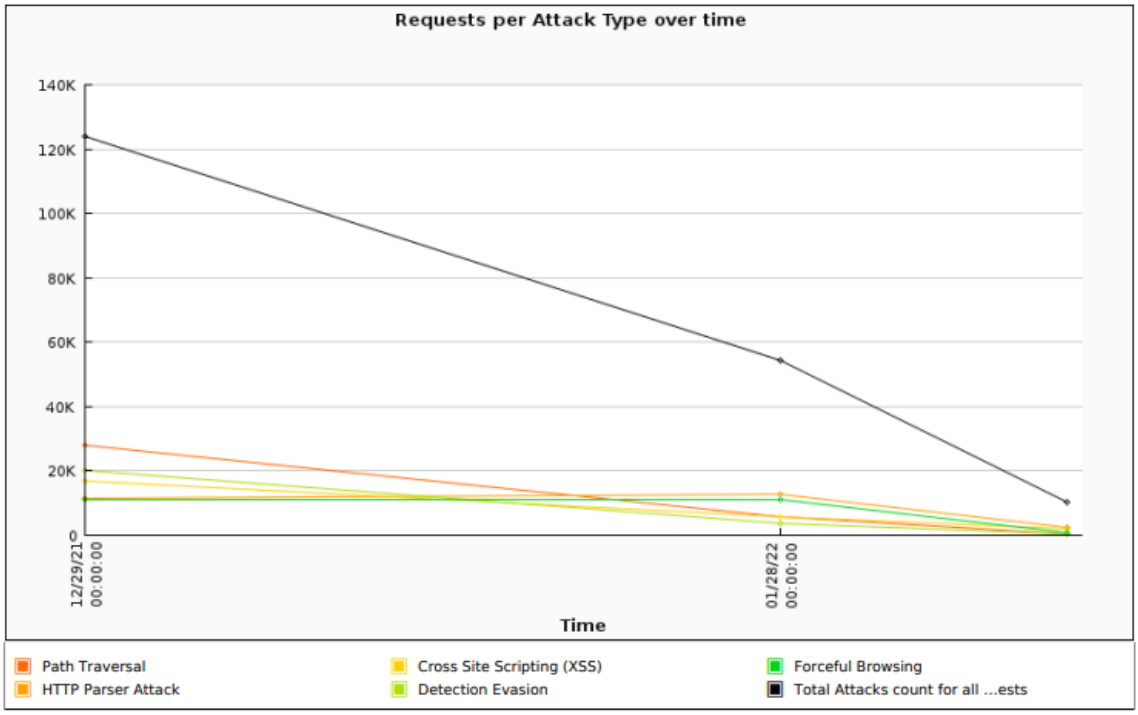


Monitoramento de tráfego SEGEP

3 ATAQUES

Durante o mês de Dezembro as tentativas de ataques bloqueados através do firewall de aplicação Web (WAF), no qual protege contra ameaças emergentes, foi no total de **188.097** (Cento e oitenta e oito mil, noventa e sete) de tentativas de ataques. E segue os top 5 tentativas de ataque:

1	Path Traversal: 33.735
2	HTTP Parser Attack: 26.695
3	Cross Site Scripting (XSS): 24.643
4	Detection Evasion: 24.040
5	Forceful Browsing: 16.951



Attack Type	▼ Requests
Path Traversal	33735
HTTP Parser Attack	26695
Cross Site Scripting (XSS)	24643
Detection Evasion	24040
Forceful Browsing	22823
Total Attacks count for all requests	188097

Também foram bloqueadas um total de **310.100** (Trezentos e dez mil e cem) 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 **66** servidores de rede, dos quais **6 (9,1%)** apresentaram **alto** nível de gravidade, **38 (57,6%)** apresentaram **médio** nível, **4 (6,1%)** apresentaram **baixo** nível, conforme classificação do OSSIM, destacando-se ainda que **0** servidores não apresentaram **nenhuma** vulnerabilidade.

Também encontramos **18 (27,3%)** 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 OSSIM detectou **363** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **14 (3,9%)** de **alto** nível, **264 (72,7%)** de **médio** nível e **85 (23,4%)** de **baixo** nível. Nos testes realizados foram identificadas diversas vulnerabilidades, entretanto não se descarta outras que porventura não foram detectadas ou que surjam futuramente.

---

[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.

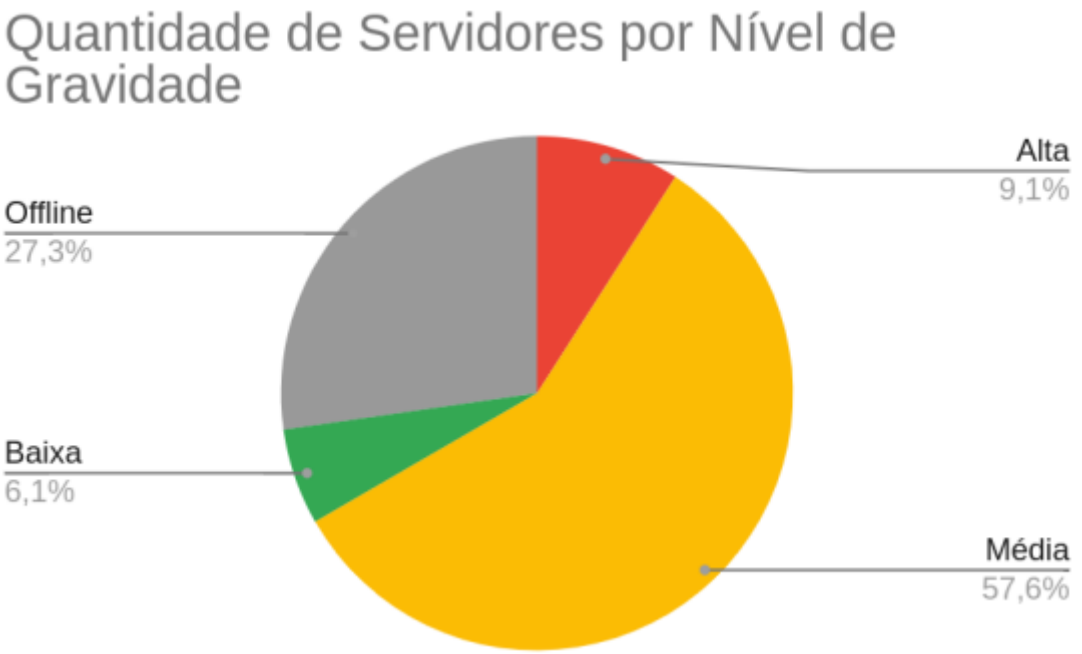
5 CONTEXTO DA ANÁLISE DE VULNERABILIDADE

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:

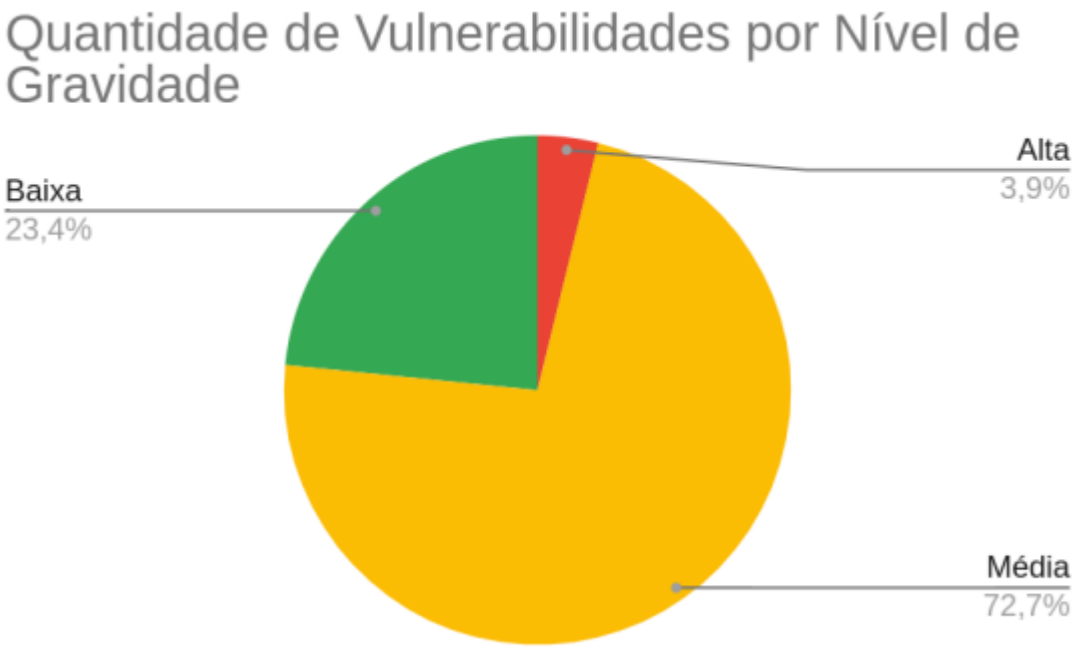
172.16.111.10 - 172.16.111.12 - 172.16.111.13 - 172.16.111.14 -
172.16.111.15 - 172.16.111.16 - 172.16.111.17 - 172.16.111.18 -
172.16.111.19 - 172.16.111.21 - 172.16.111.4 - 172.16.111.5 -
172.16.111.6 - 172.16.111.7 - 172.16.111.8 - 172.16.111.9 -
172.16.123.136 - 172.16.123.9 - 172.16.22.131 - 172.16.22.132 -
172.16.22.133 - 172.16.22.134 - 172.16.22.135 - 172.16.26.2 -
172.16.26.3 - 172.16.28.10 - 172.16.28.11 - 172.16.28.12 -
172.16.28.13 - 172.16.28.14 - 172.16.28.15 - 172.16.28.16 -
172.16.28.17 - 172.16.28.4 - 172.16.28.5 - 172.16.28.6 -
172.16.28.8 - 172.16.28.9 - 172.16.35.2 - 172.16.35.3 -
172.16.36.2 - 172.16.36.3 - 172.16.36.4 - 172.20.0.10 -
172.20.0.11 - 172.20.0.12 - 172.20.0.16 - 172.20.0.17 -
172.20.0.18 - 172.20.0.22 - 172.20.0.23 - 172.20.0.24 -
172.20.0.25 - 172.20.0.29 - 172.20.0.30 - 172.20.0.34 -
172.20.0.35 - 172.20.0.39 - 172.20.0.40 - 172.20.0.44 -
172.20.0.45 - 172.20.0.46 - 172.20.0.54 - 172.20.0.58 -
172.20.0.5 - 172.20.0.59 - 172.16.28.3

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 66 servidores de rede, dos quais 6 (9,1%) apresentaram alto nível de gravidade, 38 (57,6%) apresentaram médio nível, 4 (6,1%) apresentaram baixo nível, conforme classificação do OSSIM, destacando-se ainda que 0 servidores não apresentaram nenhuma vulnerabilidade e 18 (27,3%) endereços que não responderam, ou desligados ou inalcançáveis., conforme gráfico abaixo:



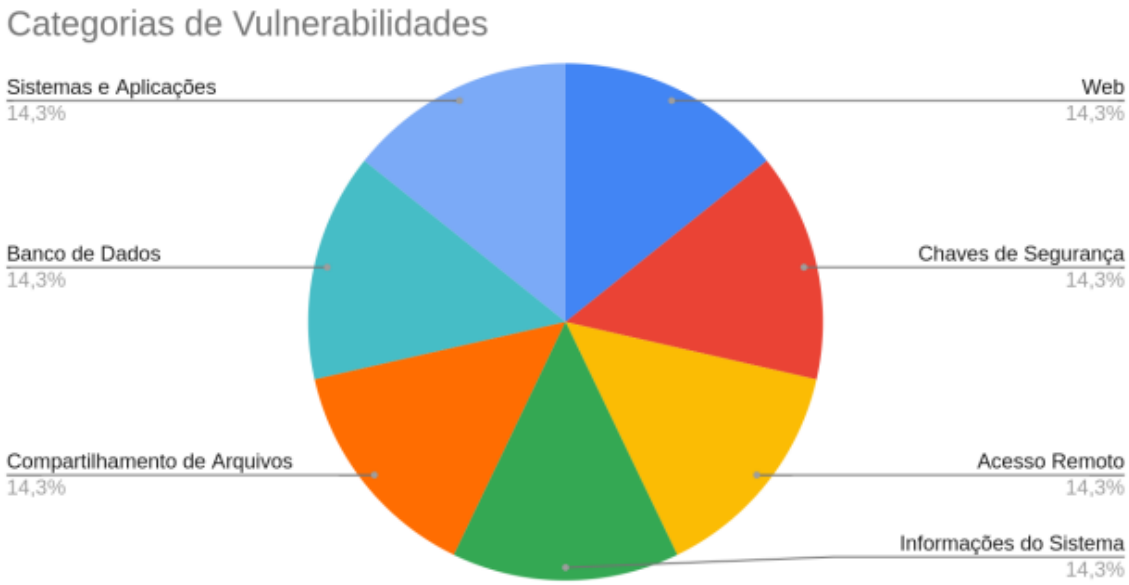
No que diz respeito às notificações apresentadas pelo OSSIM, destacam-se **363** notificações, sendo que cada uma dessas representa uma vulnerabilidade. Dentre as notificações apresentadas destacam-se: **14 (3,9%)** de **alto** nível, **264 (72,7%)** de **médio** nível e **85 (23,4%)** de **baixo** nível, 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 (16 servidores), Chaves de Segurança (49 servidores) e Informações do Sistema (53 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:

2022011546 - 2022011547 - 2022011551 - 2022011553 - 2022011555 - 2022011558 - 2022011574 - 2022011571 - 2022011559 - 2022011560 - 2022011562 - 2022011563 - 2022011582 - 2022011564 - 2022011232 - 2022011233 - 2022010480 - 2022010481 - 2022010609 - 2022010610 - 2022010920 - 2022010921 - 2022010922 - 2022010923 - 2022010924 - 2022010926 - 2022010927 - 2022010929 - 2022011000 - 2022011575 - 2022010931 - 2022010932 - 2022010935 - 2022010937 - 2022010938 - 2022010941 - 2022010944 - 2022011364 - 2022011368 - 2022010945 - 2022010947 - 2022010948 - 2022010949 - 2022010950 - 2022010951 - 2022010953 - 2022011648 - 2022011649 - 2022011651 - 2022011652 - 2022011653 - 2022011001

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 Gravid	Principais Falha	Endereço Exter	Num. Chamado	Data Chamado (	sequencia cham	Solução Apresentada no chamado
172.16.111.10	19/01/2022	1	4	2	Alta	MongoDB / SSL/	chat.sesau.ro.go	2022011546	20-01-2022 09:4	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.12	19/01/2022	0	15	0	Média	DCE/RPC / SSL/T		2022011547	20-01-2022 09:4	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.13	19/01/2022	0	4	0	Média	DCE/RPC / SSL/T	http://esus.sesa	2022011551	20-01-2022 09:4	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.14	19/01/2022	3	27	4	Alta	OS End Of Life /	hospub.cemetro	2022011553	20-01-2022 09:4	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.15	18/01/2022	5	25	4	Alta	OS End Of Life /	esus.covid19.se	2022011555	20-01-2022 09:5	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.16	19/01/2022	3	9	4	Alta	OS End Of Life /	Sistema hospub	2022011558	20-01-2022 10:0	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.17	20/01/2022	1	14	2	Alta	jQuery / Clearte	sistema.sesau.rc	2022011574	20-01-2022 11:0	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.18	20/01/2022	0	10	2	Média	DCE/RPC / SSL/T		2022011571	20-01-2022 10:2	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.19	19/01/2022	0	3	1	Média	DCE/RPC / SSL/T		2022011559	20-01-2022 10:0	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.21	20/01/2022	0	0	2	Baixa	TCP timestamps		2022011560	20-01-2022 10:0	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.4	19/01/2022						-				desligada
172.16.111.5	19/01/2022	0	21	2	Média	DCE/RPC / SSL/T	cgaf.sesau.ro.go	2022011562	20-01-2022 10:1	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.6	19/01/2022						-				desligada
172.16.111.7	19/01/2022	0	1	0	Média	SSL/TLS	-	2022011563	20-01-2022 10:1	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.8	20/01/2022	0	12	5	Média	SSH / HTTP Debu		2022011582	20-01-2022 11:2	Solicitação de cc	Encaminhado para equipe de preven
172.16.111.9	19/01/2022	0	11	1	Média	DCE/RPC / SSL/T	-	2022011564	20-01-2022 10:1	Solicitação de cc	Encaminhado para equipe de preven

IP	Data da Análise	Alta	Média	Baixa	Principal Gravid	Principais Falha	Endereço Exter	Num. Chamado	Data Chamado (	sequencia cham	Solução Apresentada no chamado
172.16.123.136	18/01/2022	0	9	1	Média	/doc directory b	sgcp.sejus.ro.go	2022011232 - 2(	17-01-2022 13:3	Atendimento a c	
172.16.123.9	10/01/2022	0	4	2	Média	HTTP Debugging	portainer-prod.s	2022010480 - 2(	07-01-2022 09:5	Atendimento a c	

IP	Data da Análise	Alta	Média	Baixa	Principal Gravid	Principais Falha	Endereço Exterr	Num. Chamado	Data Chamado (	sequencia cham	Solução Apresentada no chamado
172.16.22.131	11/01/2022	0	0	2	Baixa	TCP timestamps	-	2022010920	13-01-2022 08:2	Solicitação de cc	
172.16.22.132	11/01/2022	0	4	1	Média	DCE/RPC / SSL/T	-	2022010921	13-01-2022 08:2	Solicitação de cc	
172.16.22.133	11/01/2022	0	0	1	Baixa	TCP timestamps		2022010922	13-01-2022 08:3	Solicitação de cc	
172.16.22.134	12/01/2022	0	4	1	Média	DCE/RPC / SSL/T		2022010923	13-01-2022 08:3	Solicitação de cc	
172.16.22.135	12/01/2022	0	0	2	Baixa	TCP timestamps		2022010924	13-01-2022 08:3	Solicitação de cc	
172.16.26.2	12/01/2022	0	11	1	Média	DCE/RPC / SSL/T		2022010926	13-01-2022 08:3	Solicitação de cc	
172.16.26.3	12/01/2022	0	8	2	Média	Softbiz / IBM Prc	biblioteca.funce	2022010927	13-01-2022 08:4	Solicitação de cc	
172.16.28.10	12/01/2022					off	-				
172.16.28.11	12/01/2022	0	2	0	Média	SSH	-	2022010929	13-01-2022 08:4	Solicitação de cc	
172.16.28.12	12/01/2022	0	5	2	Média	HTTP Debugging		2022011000	13-01-2022 12:5	Solicitação de cc	
172.16.28.13	12/01/2022	0	2	2	Média	SSH / TCP timest		2022011575	20-01-2022 11:0	Solicitação de cc	
172.16.28.14	12/01/2022	0	2	2	Média	SSH / TCP timest		2022010931	13-01-2022 08:4	Solicitação de cc	
172.16.28.15	12/01/2022	0	2	2	Média	SSH / TCP timest		2022010932	13-01-2022 08:5	Solicitação de cc	
172.16.28.16	12/01/2022	0	3	1	Média	DCE/RPC / SSL/T		2022010935	13-01-2022 08:5	Solicitação de cc	
172.16.28.17	12/01/2022	0	4	1	Média	DCE/RPC / SSL/T		2022010937	13-01-2022 08:5	Solicitação de cc	
172.16.28.4	12/01/2022	0	2	2	Média	SSH / TCP timest	-	2022010938	13-01-2022 09:0	Solicitação de cc	
172.16.28.5	12/01/2022	0	2	2	Média	SSH / TCP timest	-	2022010941	13-01-2022 09:0	Solicitação de cc	
172.16.28.6	12/01/2022	0	2	2	Média	SSH / TCP timest	-	2022010944	13-01-2022 09:0	Solicitação de cc	
172.16.28.8	12/01/2022					off	-				
172.16.28.9	12/01/2022					off	-				
172.16.35.2	18/01/2022	1	4	2	Alta	MongoDB / Clea	-	2022011364	18-01-2022 11:0	Solicitação de cc	máquina legada INFOVIA
172.16.35.3	18/01/2022	0	4	3	Média	SSL/TLS / SSH / T	-	2022011368	18-01-2022 11:0	Solicitação de cc	
172.16.36.2	12/01/2022	0	2	1	Média	Cleartext Transm	-	2022010945	13-01-2022 09:1	Solicitação de cc	
172.16.36.3	12/01/2022	0	7	2	Média	Missing `httpOn	-	2022010947	13-01-2022 09:1	Solicitação de cc	
172.16.36.4	12/01/2022	0	3	0	Média	DCE/RPC / SSL/T		2022010948	13-01-2022 09:1	Solicitação de cc	

IP	Data da Análise	Alta	Média	Baixa	Principal Gravid	Principais Falha	Endereço Exterr	Num. Chamado	Data Chamado (	sequencia cham	Solução Apresentada no chamado
172.20.0.10	10/01/2022	0	2	2	Média	SSH / TCP timest		2022010949	13-01-2022 09:1	Solicitação de cc	
172.20.0.11	11/01/2022	0	2	2	Média	SSH / TCP timest		2022010950	13-01-2022 09:1	Solicitação de cc	
172.20.0.12	11/01/2022	0	2	2	Média	SSH / TCP timest		2022010951	13-01-2022 09:2	Solicitação de cc	
172.20.0.16	11/01/2022	0	2	2	Média	SSH / TCP timest		2022010953	13-01-2022 09:2	Solicitação de cc	
172.20.0.17	20/01/2022										
172.20.0.18	20/01/2022										
172.20.0.22	20/01/2022	0	2	2	Média	SSH / TCP timest		2022011648	21-01-2022 11:1	Solicitação de cc	
172.20.0.23	20/01/2022										
172.20.0.24	20/01/2022										
172.20.0.25	20/01/2022										
172.20.0.29	20/01/2022										
172.20.0.30	20/01/2022										
172.20.0.34	20/01/2022										
172.20.0.35	20/01/2022										
172.20.0.39	20/01/2022										
172.20.0.40	20/01/2022										
172.20.0.44	20/01/2022										
172.20.0.45	20/01/2022										
172.20.0.46	20/01/2022	0	2	1	Média	SSH / TCP timest		2022011649	21-01-2022 11:1	Solicitação de cc	
172.20.0.54	20/01/2022	0	3	2	Média	SSH / HTTP Debu		2022011651	21-01-2022 11:1	Solicitação de cc	
172.20.0.58 , 17	20/01/2022	0	2	2	Média	SSH / TCP timest		2022011652	21-01-2022 11:2	Solicitação de cc	
172.20.0.59	20/01/2022	0	2	2	Média	SSH / TCP timest		2022011653	21-01-2022 11:2	Solicitação de cc	
172.16.28.3	13/01/2022	0	3	2	Média	mission / SSH / T		2022011001	13-01-2022 12:5	Solicitação de cc	

Considerando as novas diretrizes da Coordenação de Segurança da Informação da SETIC, a solicitação da equipe de Data Center da Coordenação de Infraestrutura da SE

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.