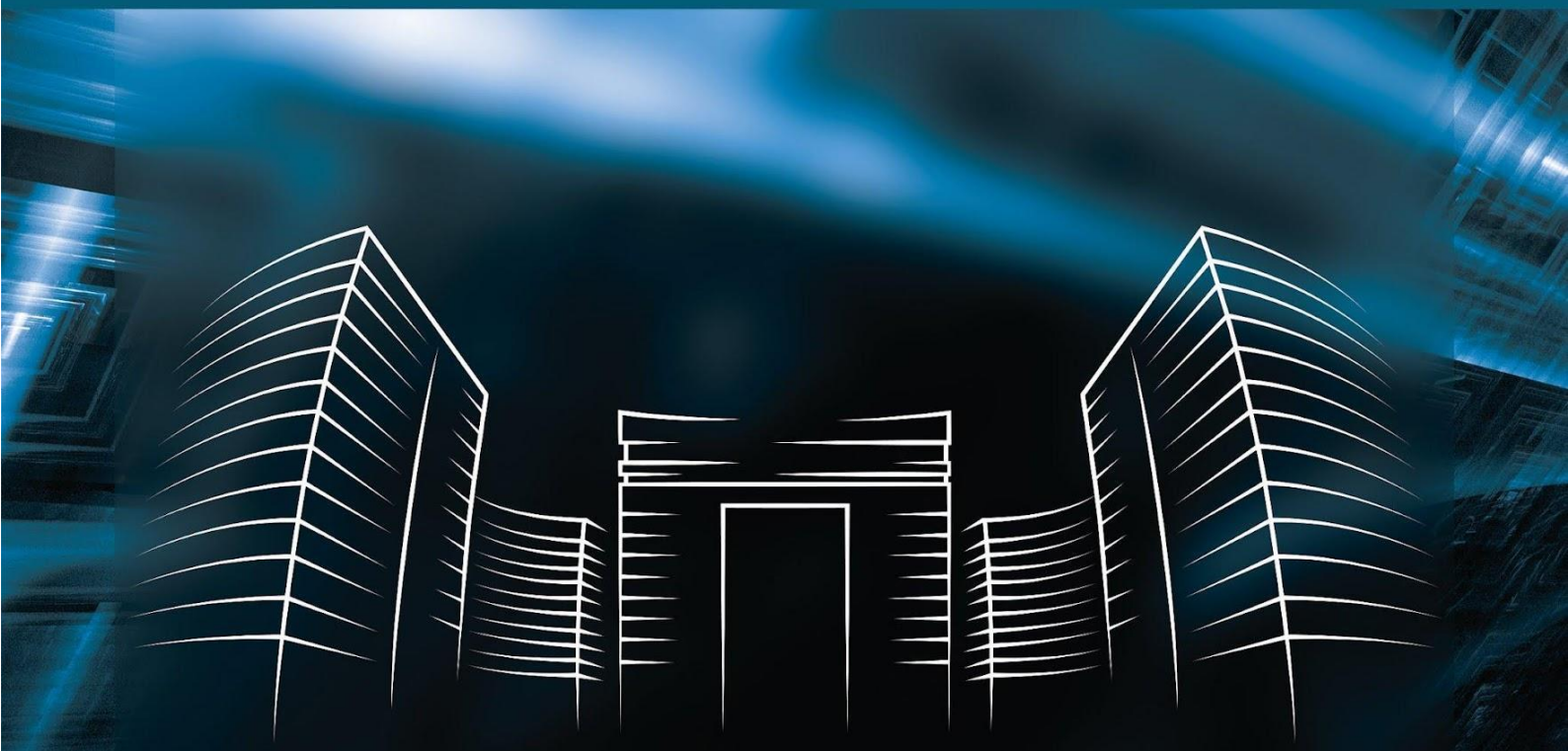
SETIC
Superintendência Estadual de Tecnologia da Informação e Comunicação

Governo do Estado de RONDÔNIA

RELATÓRIO TRIMESTRAL

Abril a Junho de 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

Rogério

Eduardo zimmer

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	05/07/2022	Rosemeire Vidal e Leonardo Courinos.	Elaboração do Relatório.

LISTA DE ABREVIATURAS

CAF	Coordenadoria de Administração e Finanças
COSEGI	Coordenadoria de Segurança da Informação
GLPI	Gestionnaire Libre de Parc Informatique
GPREV	Gerência de Prevenção de Incidentes
IPS	Intrusion Prevention System
NOC	Network Operations Center
NOPS	Núcleo de Operações
SETIC	Superintendência Estadual de Tecnologia da Informação e Comunicação
WAF	Web Application Firewall

SUMÁRIO

1 INTRODUÇÃO

A Coordenadoria de Segurança da Informação, através de diversas ações de planejamento, direcionamento de esforços e processamento de informações, busca mitigar as incertezas e alimentar a cibersegurança da SETIC, desde a coleta e obtenção de informação, do processamento da informação livre de ruído e da difusão dos resultados, de forma a permitir de maneira significativa a transformação do conhecimento aplicado à tomada de decisões e à redução de incertezas, neste contexto ligado à segurança estratégica.

Visando a manutenção contínua e garantia da ciber inteligência, a COSEGI realiza o Ciclo contínuo e análise, etapas:

1. Prever: prevê de forma proativa e transitiva os possíveis ciberataques.

2. Prevenir: realiza varreduras de vulnerabilidades fortalecendo a segurança aplicada, identificando ameaças e evitando incidentes por ciberataques.

3. Detectar: detecta incidentes de segurança, validando e priorizando os mesmos, contendo a propagação e limitando o impacto.

4. Responder: aplicação de mudanças na cibersegurança, redesenho e modificações no modelo.

Apesar do conhecimento de que garantir 100% de segurança não existe. A prevenção, detecção e resposta diante deste possível ataque é o que faz a diferença em caso de um incidente.

A COSEGI elaborou este relatório como fins de apresentação dos resultados desta coordenação durante o último trimestre (abril a junho), referente aos serviços de utilização de redes, segurança contra tentativas de ataque e análises de vulnerabilidades.

2 OPERAÇÕES DE REDE

O Núcleo de Operações de Redes é responsável por planejar, configurar, operar, controlar, monitorar e manter a estrutura física e lógica das redes sociais de comunicações da SETIC.

Utilizando ferramentas de monitoramento dos ativos de rede foi possível extrair dados que demonstram o desempenho das redes da SETIC, utilizados para compor o presente relatório.

2.1 TRÁFEGO DE REDE

Considerando os dados trafegados pelos Switches Core de Comunicação de Dados, equipamento responsável por concentrar todas as redes do Estado, originados ou destinados às estações de trabalho do Palácio Rio Madeira, unidades clientes da INFOVIA e servidores de rede hospedados no data center da SETIC, foi aferido o **volume total de 649 TB** no último trimestre.

Segue a demonstração desse resultado em número e períodos de registro de dados trafegados:

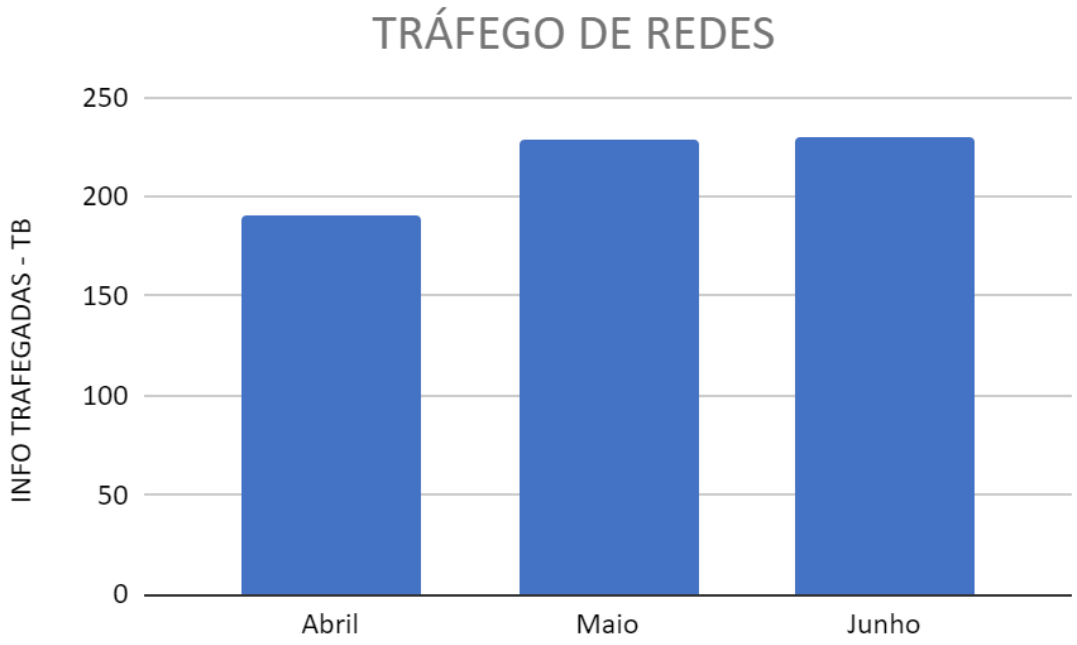


Figura 1: Demonstrativo do tráfego de redes

2.1 INTERNET

Os links de internet disponibilizados à SETIC são destinados à navegação das estações de trabalho do Palácio Rio Madeira, o acesso externo às aplicações do Governo publicadas na rede mundial de computadores.

Considerando os dados extraídos do monitoramento da comunicação dos ativos de rede da SETIC com a internet, no ano corrente foram **consumidos 203 TB de tráfego da Internet**

Segue a demonstração desse resultado em número e períodos de registro de tráfego de internet:

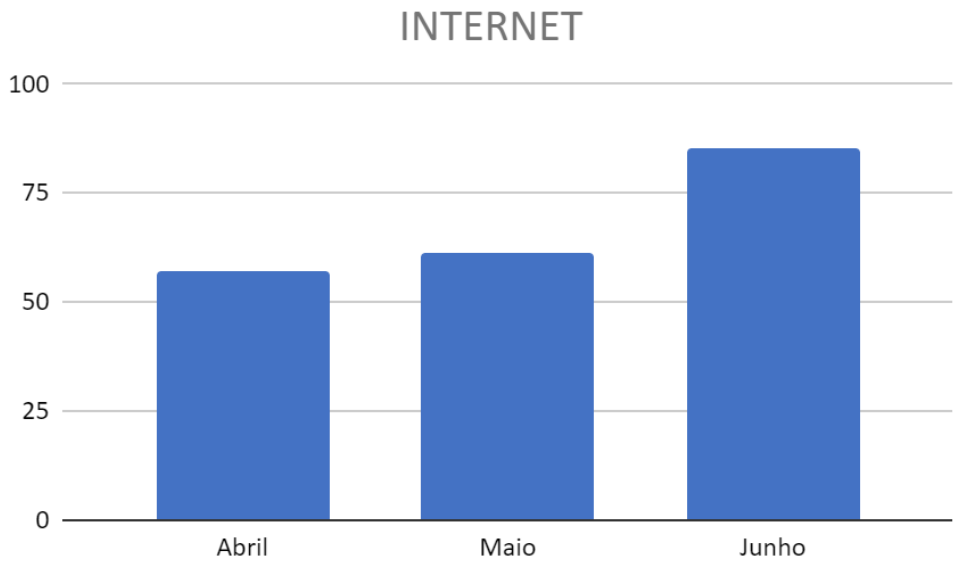


Figura 2: Demonstrativo de consumo de internet

Corrigimos as informações dos links de internet informados no relatório do primeiro trimestre do ano corrente, onde os dados extraídos do monitoramento da comunicação dos ativos de rede da SETIC com a internet foram incluídos os dados trafegados no container e a correção do mês de fevereiro. Dessa forma, o consumo do primeiro trimestre foi de **203 TB de tráfego da Internet.**

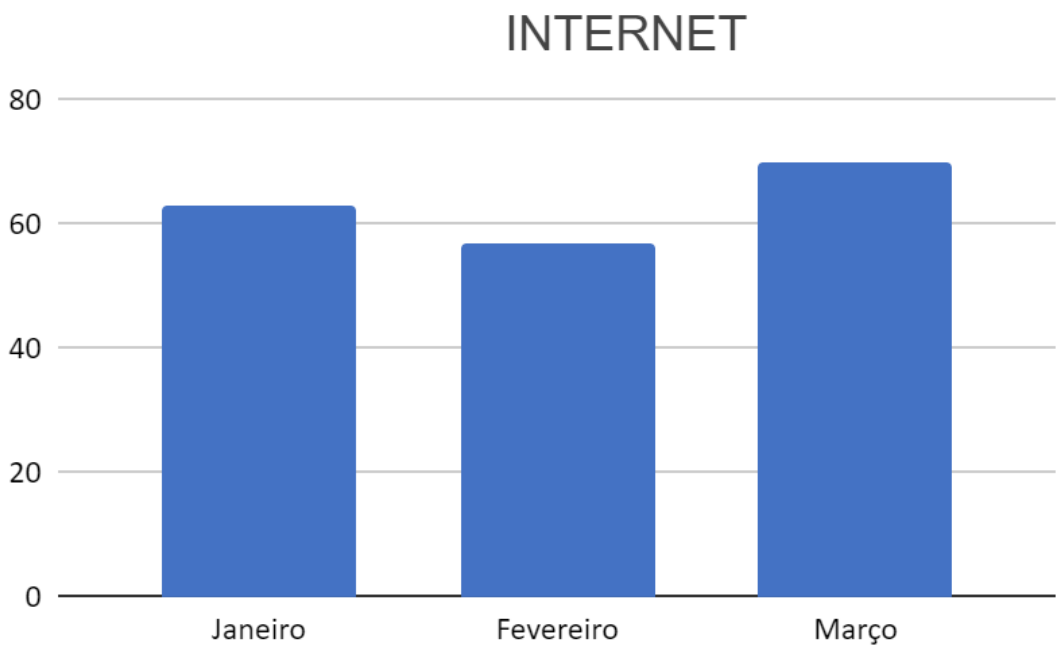


Figura 3: Demonstrativo de consumo de internet (primeiro trimestre)

No relatório deste trimestre já constam os dados trafegados no container.

3 PREVENÇÃO DE INCIDENTES

Um incidente de segurança da informação segundo a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2013, p.4):

> um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação

Sendo assim, a Gerência de Prevenção de Incidentes tem como objetivo proteger as informações mantidas pela SETIC através de ações preventivas, e em caso de ocorrência de incidentes, agir em resposta a fim de reduzir os danos causados.

A GPREVI é responsável por analisar e responder notificações e atividades relacionadas a problemas de segurança em computadores, através de análises de vulnerabilidades, testes de invasão, análise de eventos e das campanhas de conscientização interna.

3.1 TENTATIVA DE ATAQUE

Um ataque cibernético é uma ação ofensiva a fim de roubar, alterar ou destruir informações de uma organização através da obtenção de acesso não autorizado a sistemas, dispositivos ou redes.

Para garantir a confiabilidade das informações, são empregadas soluções de segurança da informação e técnicas de boas práticas. A SETIC fez aquisição de uma nova solução de Firewall e Web Application Firewall (WAF).

O Firewall é o dispositivo responsável por monitorar a entrada e saída de uma rede através da leitura de endereços e protocolos de rede trafegados por ele, aplicando regras que definem permissões e bloqueios de acesso a uma rede.

O WAF, diferente do Firewall, tem como objetivo principal a segurança de aplicações WEB, sendo assim, este dispositivo filtra os acessos às aplicações a fim de bloquear possíveis tentativas de ataque.

Considerando a compilação dos dados extraídos dos relatórios gerados pelos dispositivos de segurança da SETIC foram registrados um total de **884.246 tentativas de ataques** a sistemas e redes, sendo todas estas tentativas bloqueadas.

Abaixo segue a demonstração desse resultado em número e períodos de registro de tentativas de ataques, através de gráfico:

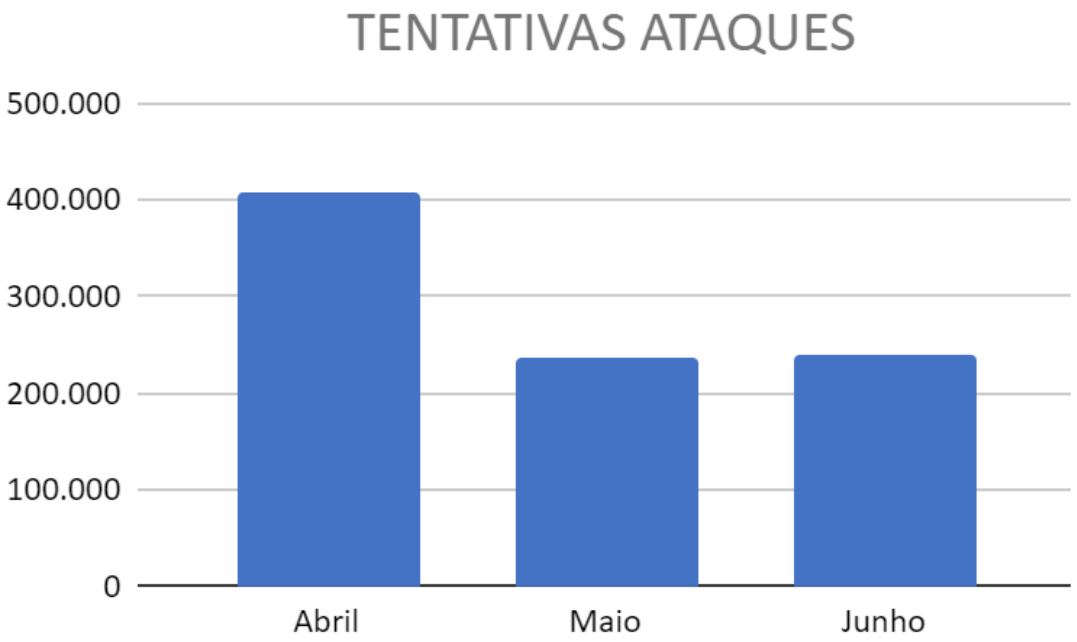


Figura 3: Demonstrativo das tentativas de ataque bloqueadas.

3.2 ANÁLISE DE VULNERABILIDADES

A definição de vulnerabilidade, em segurança da informação, segundo a ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2013, p. 11): “fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças”, ou seja, é uma fraqueza que pode ser utilizada por um atacante para ter acesso não autorizado a uma informação.

Com intuito de prevenir possíveis ataques cibernéticos, a GPREVI realiza análises nos servidores de rede hospedados na infraestrutura da SETIC, através de varreduras realizadas por um conjunto de vários serviços e ferramentas de gerenciamento de vulnerabilidades. Após a realização das análises são elaborados relatórios onde são apresentadas as vulnerabilidades detectadas assim como seus níveis de criticidade, definições e possíveis ações de solução.

Ao todo, **foram analisados 223 servidores de rede**. Importante ressaltar que nas análises é feita a classificação das vulnerabilidades encontradas em 3 diferentes níveis de gravidade: alto, médio e baixo. Destaca-se ainda que apresenta também o nível denominado “info”, que objetiva trazer informações sobre o dispositivo analisado, não sendo objeto de discussão.

No decorrer das análises dos servidores, ao todo, **foram detectadas 1.422 vulnerabilidades**. Dentre as vulnerabilidades apresentadas destacam-se: 53 (4%) de alto nível, 1.037 (73%) de médio nível e 332 (23%) de baixo nível.

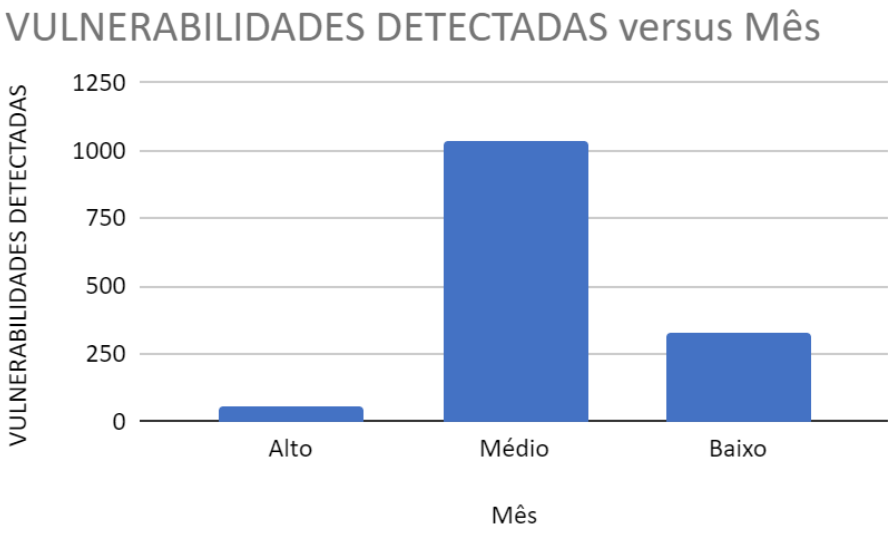


Figura 4: Demonstrativo das vulnerabilidades detectadas.

3.2.1 CATEGORÍAS DE VULNERABILIDADES

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 **Acesso Remoto (61 servidores), Chaves de Segurança (219 servidores) e Informações do Sistema (198 servidores)**, conforme observado no gráfico abaixo:

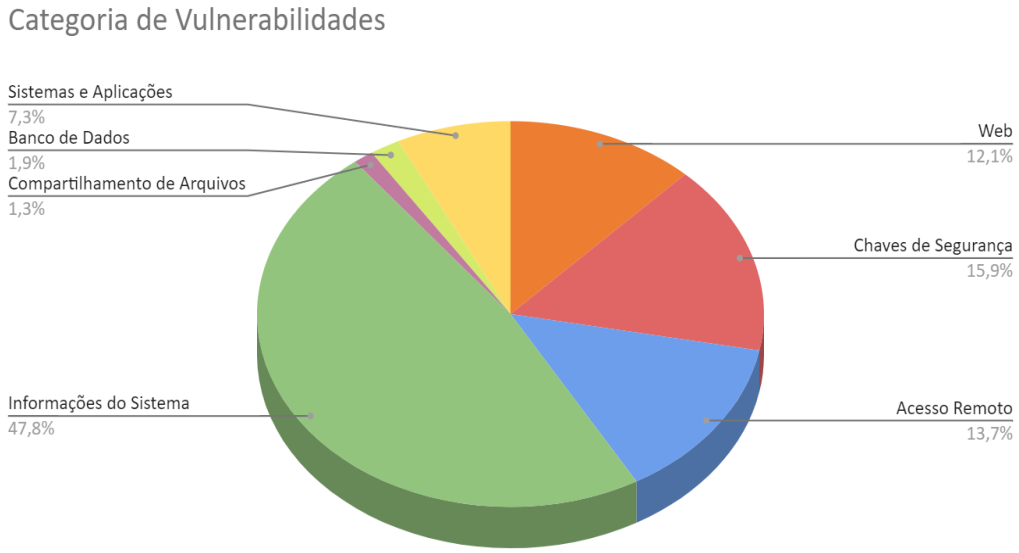


Figura 5: Demonstrativo das categorias das vulnerabilidades.

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

A vulnerabilidade é classificada de acordo com o número CVE, quanto maior o risco de invasão ou vazamento, mais crítica será a vulnerabilidade.

O Common Vulnerabilities and Exposures (CVE) é um banco de dados que registra vulnerabilidades e exposições relacionadas à segurança da informação conhecidas publicamente. O sistema é mantido pela National Cybersecurity FFRDC, operado pela Mitre Corporation, com financiamento da National Cyber Security Division do Departamento de Segurança Interna dos Estados Unidos.

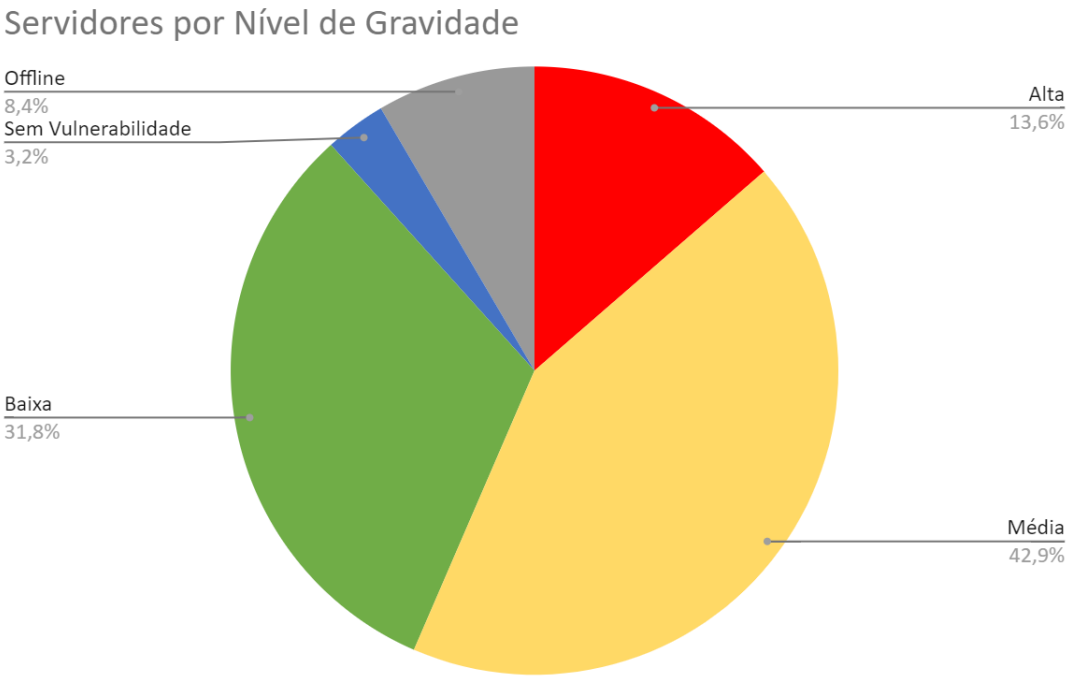


Figura 6: Demonstrativo da classificação das vulnerabilidades.

4 AÇÕES CORRETIVAS

Após a realização das análises 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:

2022061304 - 2022061305 - 2022061307 - 2022061308 - 2022061309 - 2022061315 - 2022061316 - 2022061317 - 2022061318 - 2022061319 - 2022061244 - 2022061245 - 2022061247 - 2022061259 - 2022061260 - 2022061263 - 2022061273 - 2022061274 - 2022061275 - 2022061277 - 2022061278 - 2022061280 - 2022061281 - 2022061283 - 2022061286 - 2022061300 - 2022061310 - 2022061312 - 2022061313 - 2022061327 - 2022061328 - 2022061329 - 2022061330 - 2022061331 - 2022061332 - 2022061335 - 2022061336 - 2022061337 - 2022061338 - 2022061339 -

2022061343 - 2022061345 - 2022061346 - 2022061347 - 2022061348 - 2022061349 - 2022061351 - 2022061352 - 2022061353 - 2022061324 - 2022061326 - 2022062172 - 2022062174 - 2022062194 - 2022062196 - 2022062197 - 2022062199 - 2022064946 - 2022061644 - 2022062209 - 2022062203 - 2022062205 - 2022063807 - 2022063813 - 2022063816 - 2022063822 - 2022063824 - 2022063826 - 2022063827 - 2022063828 - 2022063829 - 2022063831 - 2022063833 - 2022063837 - 2022063839 - 2022063840 - 2022063841 - 2022063842 - 2022063843 - 2022063844 - 2022063846 - 2022063847 - 2022063849 - 2022063850 - 2022063851 - 2022063508 - 2022063580 - 2022063711 - 2022064008 - 2022064972 - 2022064894 - 2022064891 - 2022064973 - 2022064974 - 2022064977 - 2022064978 - 2022064979 - 2022064980 - 2022064983 - 2022064953 - 2022064956 - 2022064958 - 2022064949 - 2022064951 - 2022064952 - 2022063971 - 2022064988 - 2022064989 - 2022065014 - 2022064988 - 2022064989 - 2022065317 - 2022065320 - 2022065321 - 2022065323 - 2022065324 - 2022065326 - 2022065401 - 2022065402 - 2022065404 - 2022065410 - 2022065411 - 2022065412 - 2022065413 - 2022065415 - 2022065416 - 2022065417 - 2022065419 - 2022065421 - 2022065422 - 2022065423 - 2022065425 - 2022065426 - 2022065427 - 2022065429 - 2022065430 - 2022065431 - 2022065432 - 2022065434 - 2022065435.

5 REFERÊNCIAS

International Organization for Standardization. **ISO/IEC 27000: Information technology — Security techniques — Information security management systems — Overview and vocabulary**. Genebra: 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001: Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos**. Rio de Janeiro: 2013.

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.

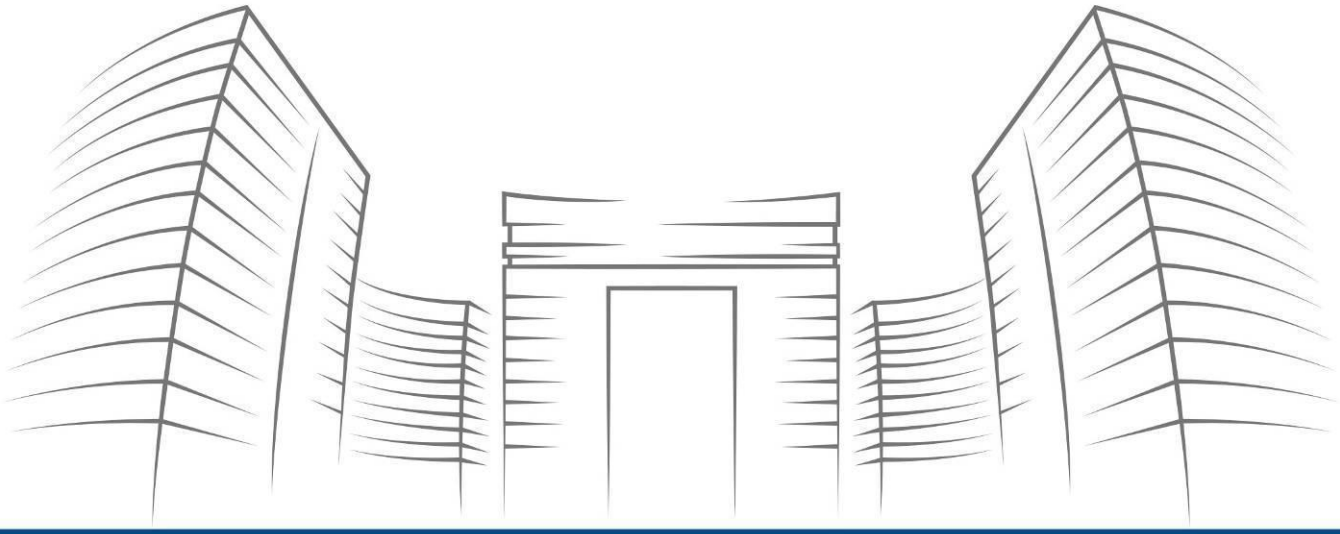
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27005: Tecnologia da informação - Técnicas de segurança - gestão de riscos de segurança da informação**. Rio de Janeiro: 2019.

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.

SETIC
Superintendência Estadual de
Tecnologia da Informação e Comunicação

Governo do Estado de
RONDÔNIA

Wiki.SETIC | *Plataforma de Documentação Operacional e Gerencial dos Serviços da SETIC*
wiki.setic.ro.gov.br



setic.ro.gov.br
@setic.rondonia

Telefone: 69 3212 9541
Endereço: Av. Farquar, 2986 - Bairro Pedrinhas
Palácio Rio Madeira, Edifício Rio Cautário - 6º Andar
Porto Velho, RO - CEP 76801470