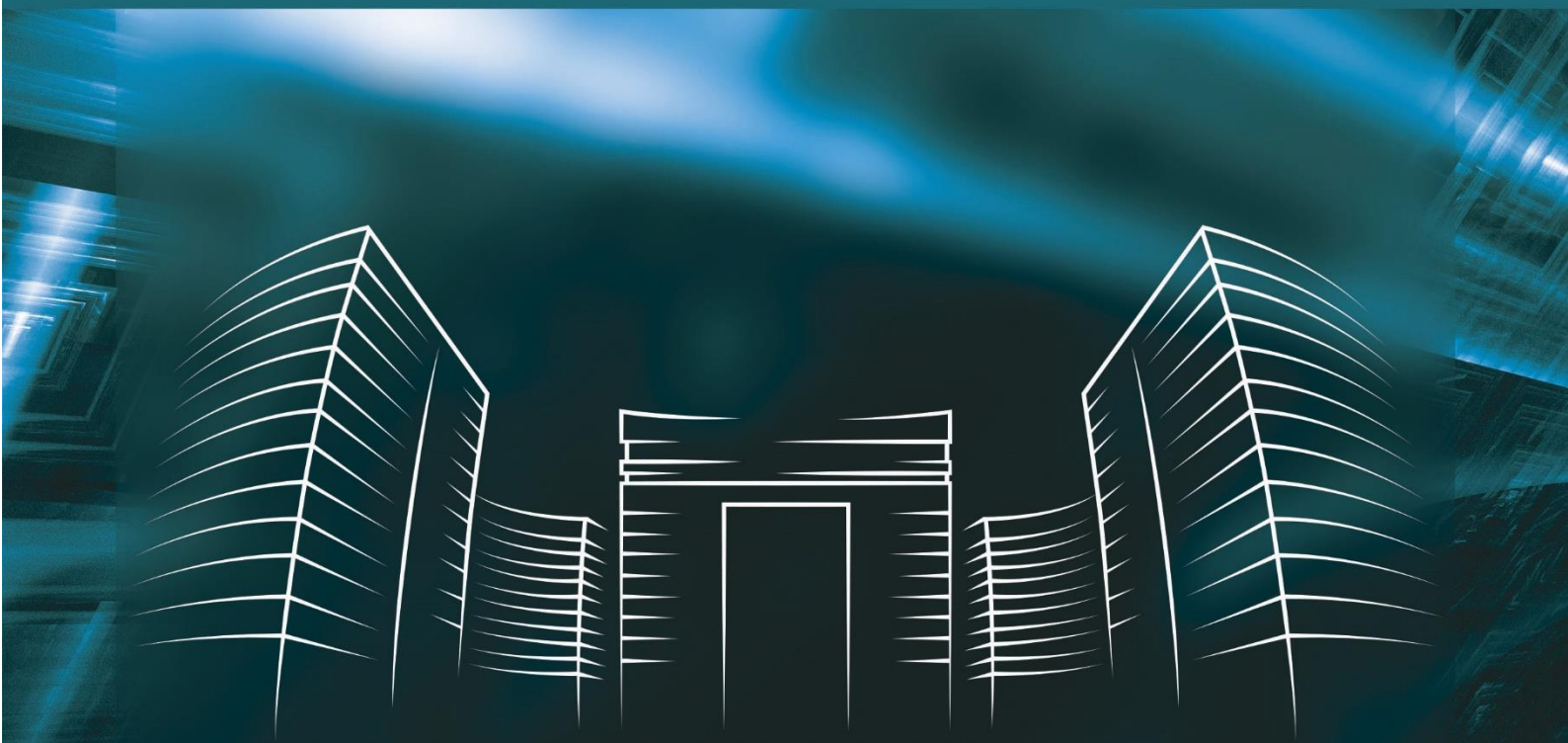
RELATÓRIO TRIMESTRAL
Julho a Setembro de 2022
COSEGI



2022

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

Delner Freire

Superintendente

Abdenildo Deividy Sobreira dos Santos

Diretor Técnico

COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Leonardo Courinos Lima da Silva

Coordenador

ELABORAÇÃO

Rosemeire Vidal da Silva

REVISÃO

Leonardo Courinos

VERSÃO

VERSÃO	DATA	AUTOR	AÇÃO
1.0	20/10/2022	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 ciber segurança 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 ciber ataques.

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

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

4. Responder: aplicação de mudanças na ciber segurança, 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 (julho a setembro), 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 518 TB** no último trimestre.

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

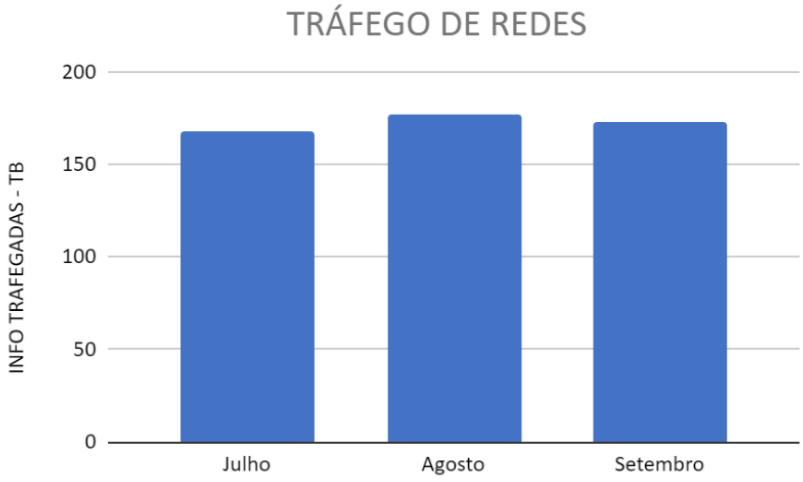


Figura 1: Demonstrativo do tráfego de redes

2.1.1 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 47 TB** de informação trafegada no mês deste relatório por secretaria.

Os dados referem-se às três maiores consumidoras deste mês de dezembro:

Secretária DER: **19 TB**

Secretária SUGESP: **15 TB**

Secretária SETIC: **13 TB**

2.2 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 160 TB de tráfego da Internet**

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

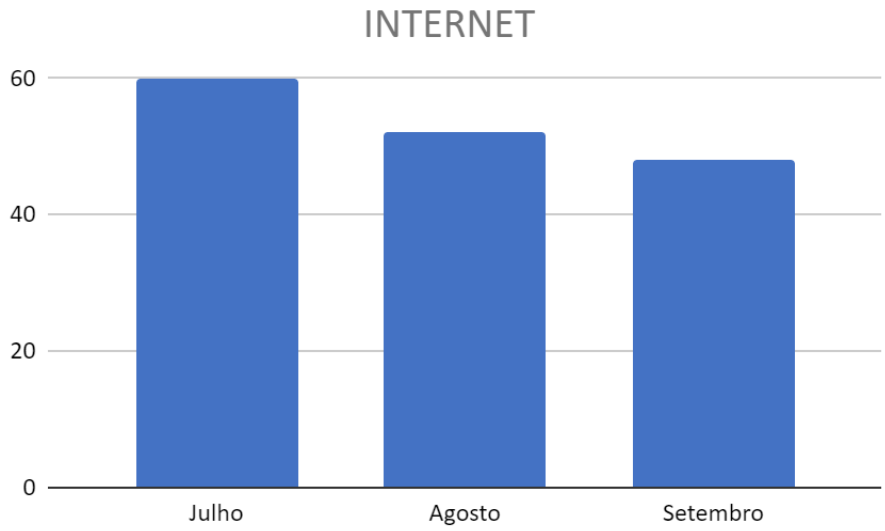


Figura 2: Demonstrativo de consumo de internet

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 conta com a 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 **823.912**

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:

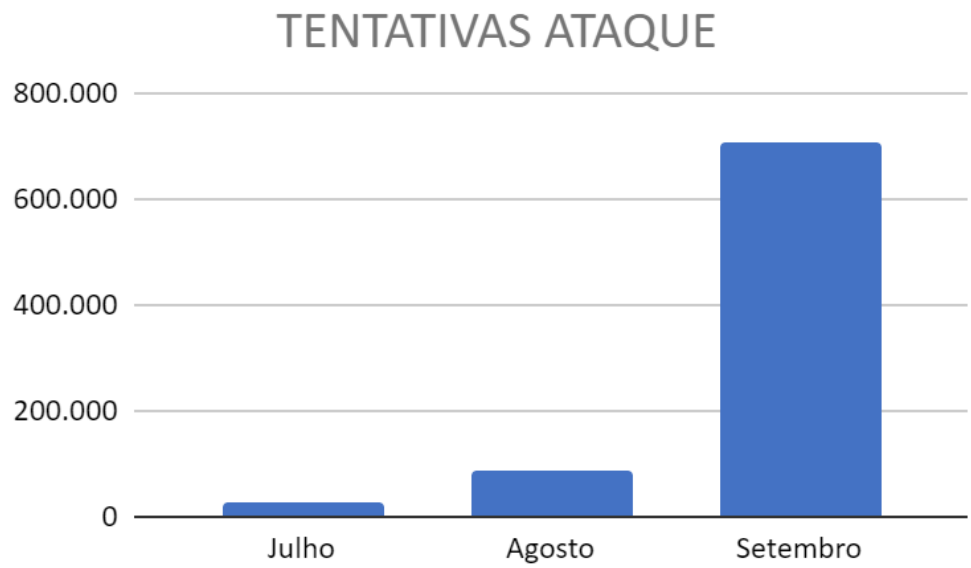


Figura 3: Demonstrativo das tentativas de ataque bloqueadas.

Houve uma baixa na quantidade de tentativas de ataque em relação ao primeiro trimestre (2.010.287 tentativas) e o segundo trimestre (1.434.024 tentativas), devido a ocorrência de queda de energia que ocasionou a desconfiguração da solução WAF e consequentemente houve uma perda de dados nos meses de julho e agosto. Realizou-se a manutenção devida, porém não foi possível restaurar os registros anteriores, apenas as configurações.

Neste período e concomitante a manutenção necessária, houve a preparação do ambiente para implantação da solução SIEM (correlação de registros de eventos), adquirido recentemente, objetivando um ambiente mais seguro, melhoria da gestão dos ativos e do gerenciamento dos registros de eventos.

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 164 (Cento e sessenta e quatro) 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, além da identificação dos servidores sem ocorrência de vulnerabilidades e dos servidores offline.

No decorrer das análises dos servidores, ao todo, **foram detectadas 938 (Novecentos e trinta e oito) vulnerabilidades**. Dentre as vulnerabilidades apresentadas destacam-se: 48 (9,8%) de alto nível, 756 (53%) de médio nível e 134 (6,7%) de baixo nível. Além de 8,5% identificados "Sem Vulnerabilidade e 22% identificados como "Offline".

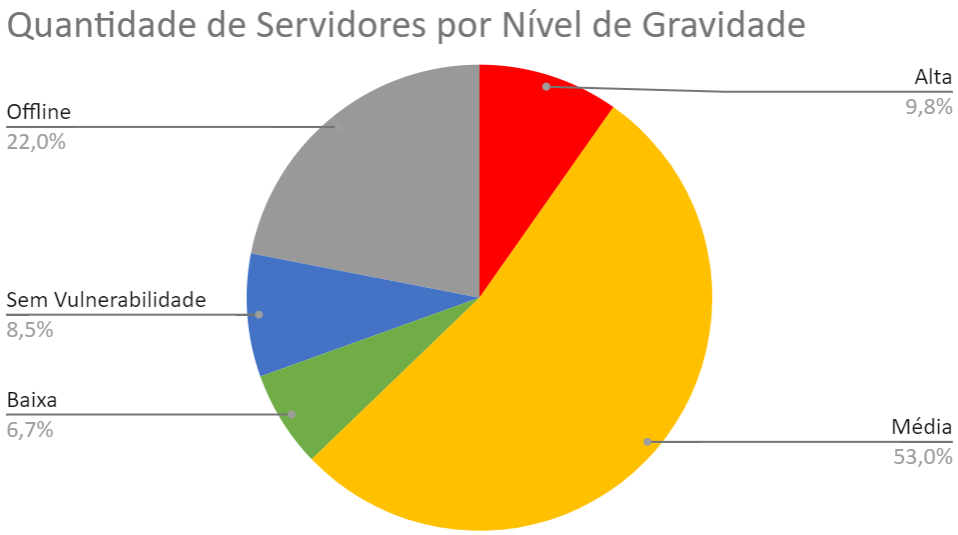


Figura 4: Demonstrativo das vulnerabilidades detectadas.

3.2.1 CATEGORIAS 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 (44 servidores), Chaves de Segurança (115 servidores) e Informações do Sistema (76 servidores)**, conforme observado no gráfico abaixo:

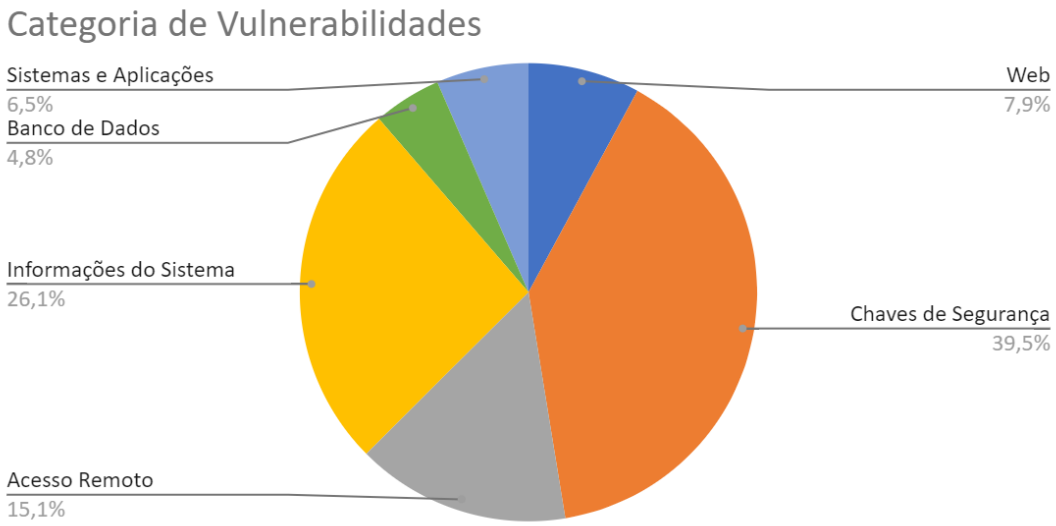


Figura 5: Gráfico de vulnerabilidade.

4 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.

Governo do Estado de

RONDÔNIA