CIBERSEGURIDAD
Universidad Nacional del Comahue

Plataforma de visualización y monitoreo de Seguridad

Sumario

1. Introducción general

La plataforma de visualización y monitoreo se implementa utilizando Grafana, la cual permite consolidar y presentar información técnica compleja de forma clara y estructurada mediante paneles y visualizaciones.

En este contexto, la plataforma cumple un rol de visualización y centralización de datos, sin generar información propia, integrando fuentes internas y externas gestionadas por el Área de Ciberseguridad.

Los datos presentados en la plataforma deben interpretarse dentro de su contexto técnico y operativo. La existencia de alertas, vulnerabilidades o reportes externos no implica necesariamente un incidente activo ni compromiso efectivo de los sistemas.

La validación y priorización corresponde a los equipos técnicos responsables junto al Área de Ciberseguridad.

Cada panel está diseñado para facilitar la interpretación de la información y la priorización de tareas de seguridad, evitando conclusiones erróneas o interpretaciones fuera de contexto.

La plataforma está concebida como una herramienta de apoyo a la gestión técnica y a la toma de decisiones, y no como un sistema de control disciplinario.

La información mostrada en los paneles proviene de

- Reportes internos de monitoreo
- Reportes externos de terceros
- Información de inteligencia de amenazas (listas negras, reputación, abusos)
- Resultados de evaluaciones técnicas periódicas

Todos los datos presentados pasan por procesos de normalización, validación y correlación, con el objetivo de reducir falsos positivos y facilitar la toma de decisiones.

Esta integración permite contar con una visión centralizada, coherente y verificable del estado de seguridad de la infraestructura institucional.

Estructura general de los paneles:

En la parte superior de los paneles se encuentra el filtro de red o IP (ip_filter), que permite definir el conjunto de activos que se desean visualizar, pudiendo seleccionarse un host individual o la red completa.

Asimismo, la plataforma dispone de un selector de rango temporal, que permite establecer el período de tiempo sobre el cual se desea consultar la información.

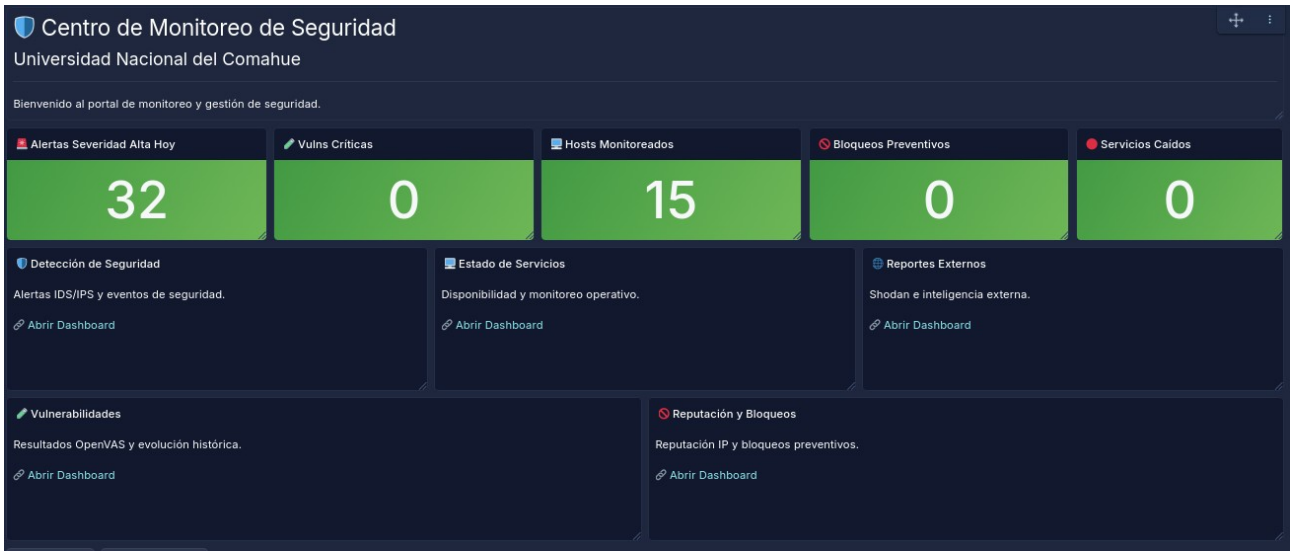
Ambos elementos —el filtro de red/IP y el rango temporal— actúan de forma conjunta y determinan qué datos se muestran en cada panel, recalculándose todas las métricas y visualizaciones en función de los valores seleccionados.

Los paneles disponibles son los siguientes:

2. Inicio

Al ingresar al portal de monitoreo, el usuario visualizará el dashboard principal del Centro de Monitoreo de Seguridad.

Esta pantalla funciona como punto central de acceso a los distintos módulos operativos y permite visualizar rápidamente el estado general de la infraestructura y de los eventos de ciberseguridad.



2.1. Indicadores superiores

La fila superior presenta indicadores resumidos que muestran el estado actual del entorno monitoreado que corresponden a los activos o rangos IP asociados al área o dependencia.

- Cantidad de Alertas Severidad Alta Hoy.
- Vulnerabilidades Críticas.
- Hosts Monitoreados
- Bloqueos Preventivos
- Servicios Caídos

2.2 La sección inferior

Contiene accesos directos a dashboards especializados.
Cada sección permite profundizar el análisis sobre un área específica.

3. Detección de Seguridad

El dashboard Detección de Seguridad centraliza los eventos generados por las herramientas IDS/IPS utilizadas en la infraestructura institucional. La severidad de las alertas corresponde a la clasificación definida por las reglas IDS y debe interpretarse como un indicador técnico orientativo.

Su objetivo es brindar una vista rápida del estado de seguridad, permitiendo identificar:

- intentos de intrusión,
- comportamientos anómalos,
- eventos de red sospechosos,
- y tendencias de actividad detectadas por los sensores.

3.1 Resumen principal

La fila superior muestra indicadores generales del período seleccionado.

- Total Alertas
- Alertas Severidad Alta
- IPs Atacantes Únicas
- Firmas/Alertas Detectadas
- IPs Destino Atacadas

3.2 Tendencias y distribución

Alerta en tiempo por severidad : El gráfico temporal muestra cómo evolucionan las alertas de seguridad a lo largo del tiempo.

Permite detectar:

- picos de actividad,
- campañas específicas,
- horarios de mayor actividad maliciosa.

Distribución por protocolo: Muestra qué protocolos generan mayor cantidad de eventos.

Ejemplos comunes:

- TCP
- UDP
- ICMP

Esto ayuda a identificar: tipos de tráfico predominantes, ataques de red y exploraciones automatizadas.

3.3 Top atacantes y servicios

Top IPs origen atacantes: Es un listado de las direcciones IP externas que generaron mayor cantidad de alertas.

Permite identificar atacantes recurrentes, detectar scanners y evaluar necesidad de bloqueo preventivo.

Servicios más atacados: Permite identificar cuáles son los servicios o aplicaciones que reciben mayor cantidad de eventos detectados por el IDS.

Top firmas / amenazas: Representación gráfica de las amenazas más frecuentes observadas durante el período.

Facilita identificar rápidamente:

- tendencias,
- tipos de ataque predominantes,
- eventos recurrentes.

3.4 IPs propensas a ataques

El panel IPs propensas a ataques permite identificar activos internos que presentan mayor exposición o concentración de eventos de seguridad.

El objetivo es priorizar análisis y acciones preventivas sobre los equipos que muestran mayor riesgo operativo o de seguridad.

3.5 Incidentes Detectados (detalle)

El panel Incidentes Detectados (detalle) presenta el registro detallado de los eventos de seguridad identificados por el IDS/IPS durante el período seleccionado.

Es uno de los paneles más importantes para análisis operativo, ya que permite visualizar cada incidente individualmente y realizar investigaciones específicas sobre actividad sospechosa o maliciosa.

4. Estado de Servicios

El Panel Estado de Servicios presenta información sobre la disponibilidad y el estado operativo de los servicios y hosts monitoreados.

Su objetivo es brindar visibilidad sobre interrupciones, degradaciones y recuperaciones de servicios críticos, permitiendo una detección temprana de fallas y un seguimiento de eventos recientes.

Los servicios y hosts incluidos en este Panel se incorporan al monitoreo a solicitud del técnico responsable, en función de la criticidad del servicio, su exposición y las necesidades operativas definidas por cada área.

4.1 Resumen

La fila superior presenta indicadores resumidos que muestran el estado actual del entorno monitoreado:

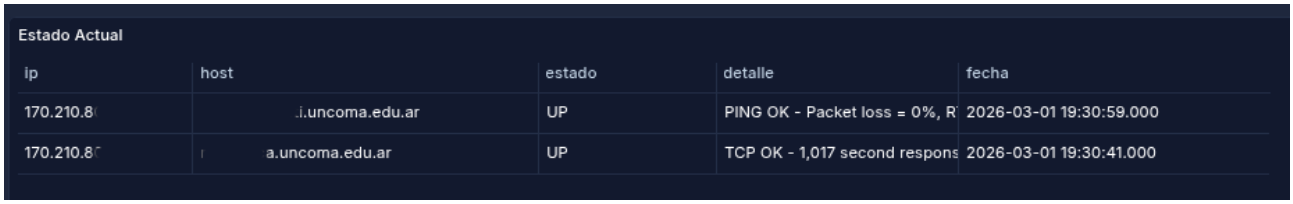
- Total de Host Monitoreados
- Host UP
- Host Down
- Total de Eventos
- Caidas en el Período

4.2 Estado actual del servicio

Esta visualización muestra el estado actual de los servicios y hosts monitoreados al momento de la consulta.

Los estados reflejan la condición operativa informada por el sistema de monitoreo y permiten identificar rápidamente servicios caídos, con fallas intermitentes o funcionando con normalidad.

Se utiliza para el seguimiento operativo, detección de caídas activas y validación posterior a tareas de mantenimiento



Estado Actual

ip	host	estado	detalle	fecha
170.210.8	.i.uncoma.edu.ar	UP	PING OK - Packet loss = 0%, R	2026-03-01 19:30:59.000
170.210.8	a.uncoma.edu.ar	UP	TCP OK - 1,017 second respons	2026-03-01 19:30:41.000

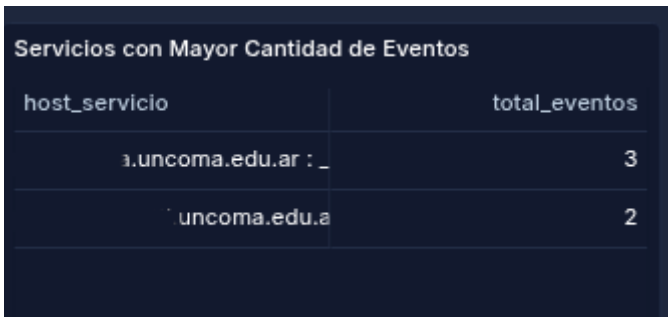
4.3 Servicios con mayor cantidad de eventos

Esta visualización presenta un ranking de los servicios que registraron la mayor cantidad de eventos dentro del período y alcance seleccionados.

Cada evento corresponde a un cambio de estado o notificación generada por el sistema de monitoreo, incluyendo caídas, recuperaciones o estados de advertencia.

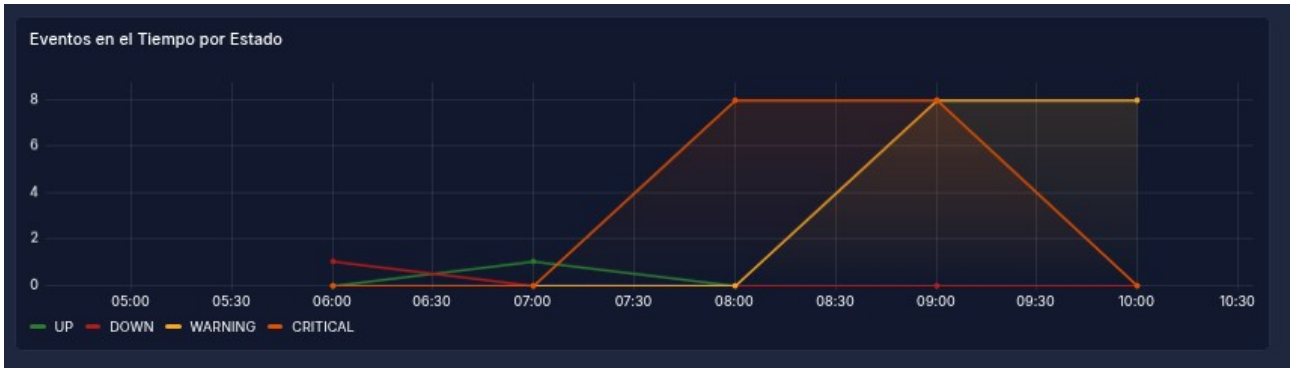
El objetivo de esta visualización es identificar servicios inestables o con comportamientos recurrentes, que pueden requerir una revisión técnica más profunda, ajustes de configuración o acciones correctivas preventivas.

La información presentada permite diferenciar incidentes puntuales de problemas persistentes, contribuyendo a la priorización de tareas de mantenimiento y mejora de la disponibilidad



4.4 Eventos en el Tiempo por Estado

Este Panel muestra la evolución temporal del estado de los servicios monitoreados. Su objetivo es permitir visualizar cómo varía la disponibilidad y el comportamiento operativo de los servicios a lo largo del tiempo.

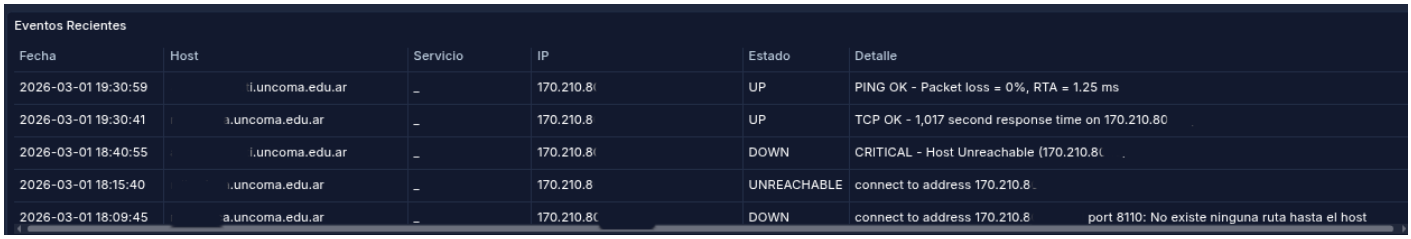


4.5 Eventos recientes del servicio

La visualización Eventos recientes del servicio presenta un historial cercano de cambios de estado, incluyendo caídas y recuperaciones de servicios monitoreados.

Su objetivo es brindar contexto temporal sobre incidentes recientes, permitiendo identificar interrupciones breves, fallas recurrentes o recuperaciones automáticas.

Esta visualización es especialmente útil para analizar comportamientos intermitentes y para validar acciones correctivas realizadas por los equipos técnicos.



5. Reportes Externos

El dashboard Reportes Externos consolida información proveniente de fuentes externas de inteligencia y monitoreo de Internet, permitiendo identificar incidentes observados desde fuera de la infraestructura institucional.

Su objetivo es complementar el monitoreo interno incorporando una visión externa sobre:

- exposición de servicios,
- configuraciones inseguras,
- actividad sospechosa,
- y posibles indicadores de compromiso detectados por terceros.

5.1 Resumen del periodo

La fila superior muestra indicadores generales correspondientes al período seleccionado.

- Total Reportes : Cantidad total de incidentes o eventos reportados por las fuentes externas. Representa el volumen general de observaciones realizadas sobre activos institucionales.
- Críticos: Cantidad de reportes clasificados con severidad crítica.
- Altos: Cantidad de eventos de severidad alta detectados externamente.
- IPs Afectadas : Cantidad de direcciones IP institucionales involucradas en reportes externos.
- Fuentes Distintas : Cantidad de fuentes externas diferentes que generaron reportes.
- Familias / Tipos Detectados: Cantidad de categorías o tipos de incidentes identificados.

5.2 Distribución y Línea de Tiempo

Gráfico temporal que muestra la evolución de incidentes externos según nivel de severidad.

Permite:

- identificar tendencias,
- detectar picos de exposición,
- evaluar recurrencia de incidentes.

Distribución por severidad: Representación porcentual de incidentes clasificados por severidad.

5.3 Top Fuentes, Familias y Puertos

Muestra IPs reportadas, cantidad de incidentes, familias detectadas, servicios asociados y score de exposición.

Ayuda a identificar:

- activos más expuestos
- servicios recurrentemente reportados,
- principales superficies de ataque.
- Top puertos reportados

5.4 Score de exposición por IP

Panel de correlación que asigna un puntaje de exposición o riesgo según: cantidad de incidentes, severidad, tipos detectados, recurrencia.

El score facilita la priorización de revisiones técnicas y análisis preventivos.

5.5 Detalle de reportes externos

Muestra una tabla detallada con cada incidente reportado, incluyendo fecha, IP afectada, puerto, protocolo, severidad y tipo de amenaza.

6. Vulnerabilidades

El dashboard Vulnerabilidades tiene como objetivo central mostrar el estado actual de exposición de los activos monitoreados, facilitando la priorización de remediaciones y el seguimiento de riesgos técnicos detectados sobre la infraestructura institucional. La presencia de una vulnerabilidad no implica necesariamente explotación activa ni compromiso del sistema, sino la detección de una condición técnica potencialmente riesgosa.

La información presentada proviene principalmente de herramientas de análisis de vulnerabilidades y mide exposición técnica y estado de vulnerabilidades detectadas.

Este dashboard permite:

- visualizar el estado actual de exposición,
- identificar activos con mayor riesgo,
- priorizar tareas de remediación,
- realizar seguimiento histórico,
- detectar configuraciones inseguras,
- evaluar evolución del riesgo técnico.

6.1 Resumen del estado actual

La fila superior presenta indicadores generales correspondientes al último estado relevado.

Total Hallazgos: Cantidad total de vulnerabilidades detectadas actualmente.

Critical: Cantidad de vulnerabilidades críticas detectadas, Estas vulnerabilidades requieren atención prioritaria debido a su alto impacto potencial.

High: Cantidad de vulnerabilidades de severidad alta.

Medium: Cantidad de vulnerabilidades medias detectadas.

Low / Log: Cantidad de hallazgos informativos o de bajo impacto.

IPs Escaneadas: Cantidad de activos incluidos en el último análisis de vulnerabilidades.

6.2 Distribución y score

Distribución por nivel: Gráfico porcentual que muestra la distribución de vulnerabilidades según severidad.

Vulnerabilidades por IP — Critical + High

Tabla que identifica los activos con vulnerabilidades de mayor severidad, permite identificar activos críticos.

CVSS promedio del equipo: Indicador consolidado del nivel promedio de riesgo técnico detectado.

El cálculo se basa en el score CVSS (Common Vulnerability Scoring System).

Interpretación general:

0–3 → Bajo

4–6 → Medio

7–8 → Alto

9–10 → Crítico

Un valor elevado indica mayor exposición técnica promedio sobre los activos evaluados.

6.3 Top vulnerabilidades

Top 10 Vulnerabilidades más frecuentes: Muestra las vulnerabilidades o plugins de detección más repetidos durante el último análisis.

Permite identificar: problemas recurrentes, debilidades estructurales y patrones de configuración.

Top 10 puertos vulnerables: Visualización de los puertos asociados a mayor cantidad de vulnerabilidades detectadas.
Ayuda a identificar servicios más expuestos y superficies de ataque.

6.4 Score de riesgo por host

Tabla consolidada de riesgo técnico por activo.

Relaciona: cantidad de vulnerabilidades, severidad, score CVSS, fecha del último análisis y score consolidado.

Permite priorizar: remediaciones, revisiones técnicas y análisis preventivos.

6.5 Detalle de hallazgos

Listado detallado de vulnerabilidades detectadas en el último análisis.

Generalmente incluye:

- IP afectada,
- puerto,
- protocolo,
- severidad,
- score CVSS,
- nombre de vulnerabilidad,
- solución recomendada.

Esta sección se utiliza principalmente para: análisis técnico, planificación de remediaciones y seguimiento operativo.

7. Consideraciones finales

La plataforma centraliza información técnica proveniente de múltiples fuentes de monitoreo, detección y análisis, permitiendo mejorar la visibilidad sobre el estado de seguridad y disponibilidad de los servicios institucionales.

La información presentada constituye una herramienta de apoyo para la gestión técnica, el análisis operativo y la priorización de tareas de remediación y monitoreo.

Los datos visualizados deben interpretarse dentro de su contexto técnico y operativo, considerando que la existencia de alertas, vulnerabilidades o reportes externos no implica necesariamente un incidente activo ni un compromiso efectivo de los sistemas.

La validación, análisis y definición de acciones correctivas corresponde a los equipos técnicos responsables junto al Área de Ciberseguridad, en función de la criticidad, impacto y contexto de cada situación detectada.