**EMPRESA CDA DEL VALLE**
**CONTRATO N.°: CDAV-079-2026**
**INFORME DE ACTIVACIÓN DE WAZUH Y NETGATE PFSENSE**
**ABRIL 30 DEL 2026**

1. **Objeto del Contrato**

   El presente contrato tiene como finalidad la provisión e implementación de una solución integral de infraestructura tecnológica basada en:

   - **Netgate:** Dispositivo firewall **pfSense** para gestión de seguridad y conectividad de red.

   - **Wazuh:** Plataforma de seguridad de código abierto utilizada para la detección de amenazas, monitoreo de integridad, análisis de logs y respuesta ante incidentes (SIEM/XDR) en infraestructuras IT. Cuenta con suscripción de soporte profesional, que brinda asistencia técnica especializada, actualizaciones priorizadas y acompañamiento para la correcta implementación, operación y optimización de la solución.

2. **Estado Actual del Contrato**

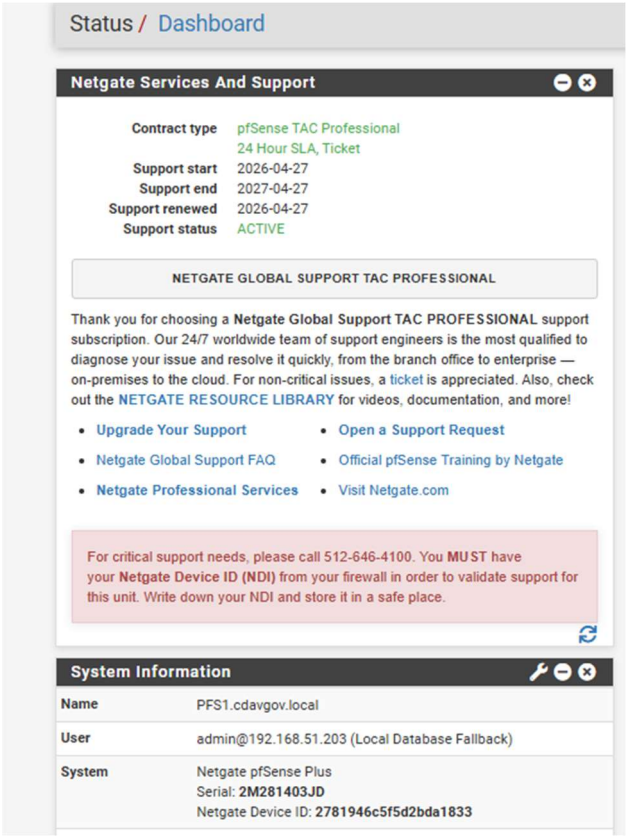
   - **Fase del proyecto:** Finalizada
   - **Estado del sistema:** Estable
   - **Actividad actual:** Activación de plataformas.
   - **Cumplimiento del contrato:** Sí

3. **Resumen de activación de plataformas**

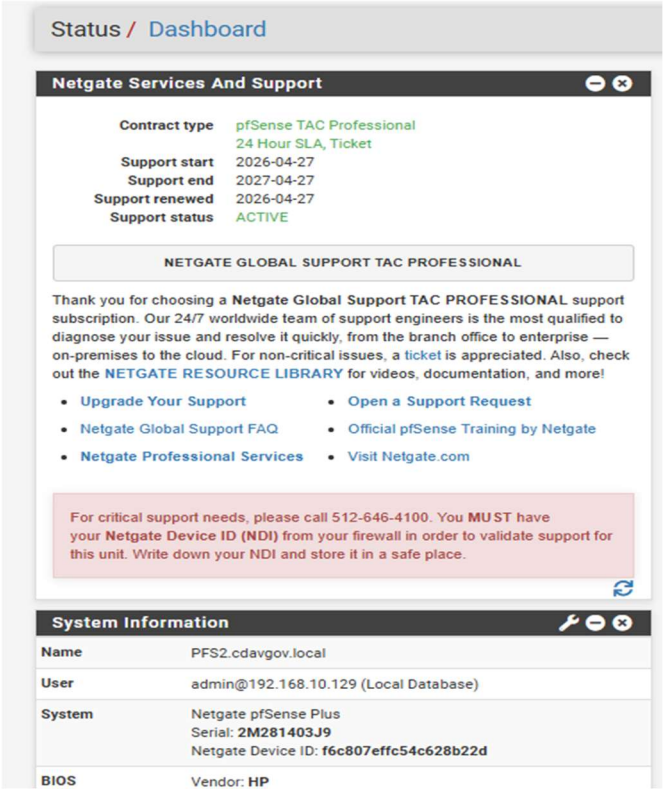
   Durante el procedimiento en compañía del ingeniero Hernan Rodrigo Bedoya y Julian Arango de Soluciones en seguridad informática, se verifica que la operatividad, el servicio adquirido están disponibles y activos:

   - **Netgate (pfSense):**

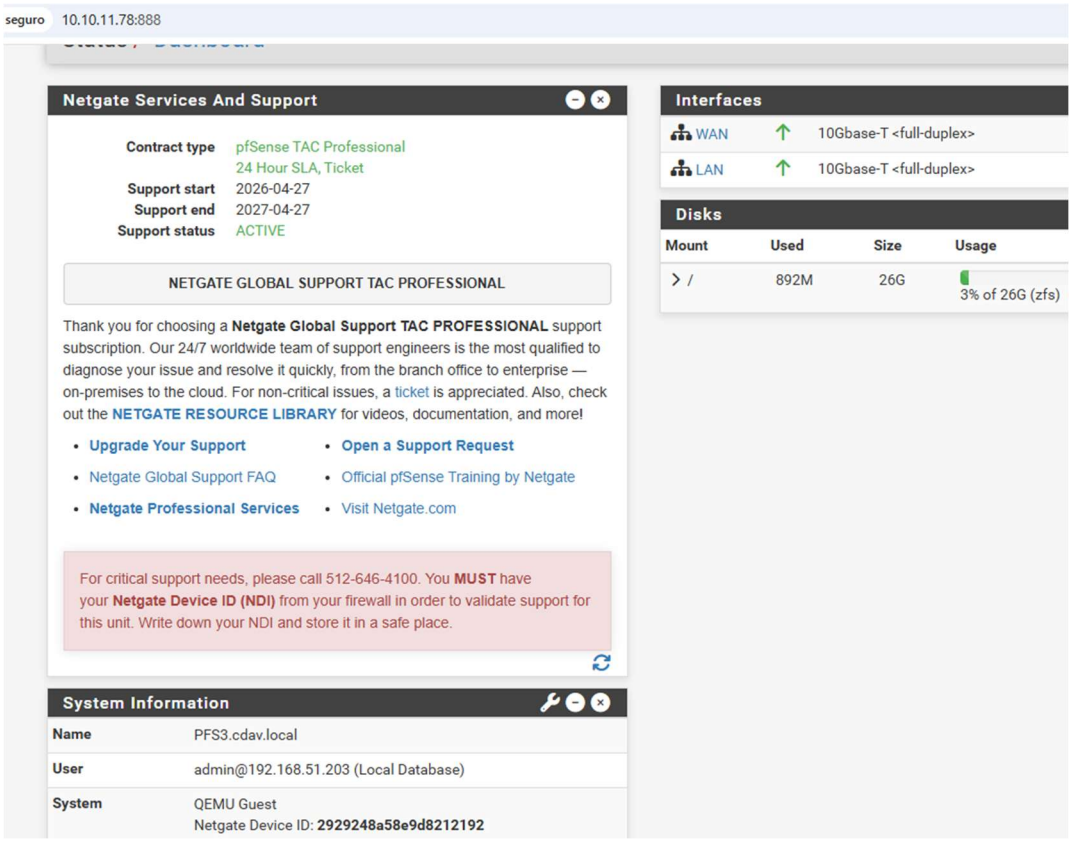
- **PFS-1**


Status / Dashboard
Netgate Services And Support
Contract type pfSense TAC Professional
24 Hour SLA, Ticket
Support start 2026-04-27
Support end 2027-04-27
Support renewed 2026-04-27
Support status ACTIVE
NETGATE GLOBAL SUPPORT TAC PROFESSIONAL
Thank you for choosing a Netgate Global Support TAC PROFESSIONAL support subscription. Our 24/7 worldwide team of support engineers is the most qualified to diagnose your issue and resolve it quickly, from the branch office to enterprise — on-premises to the cloud. For non-critical issues, a ticket is appreciated. Also, check out the NETGATE RESOURCE LIBRARY for videos, documentation, and more!
Upgrade Your Support
Open a Support Request
Netgate Global Support FAQ
Official pfSense Training by Netgate
Netgate Professional Services
Visit Netgate.com
For critical support needs, please call 512-646-4100. You MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place.
System Information
Name PFS1.cdavgov.local
User admin@192.168.51.203 (Local Database Fallback)
System Netgate pfSense Plus
Serial: 2M281403JD
Netgate Device ID: 2781946c5f5d2bda1833

- **PFS-2**

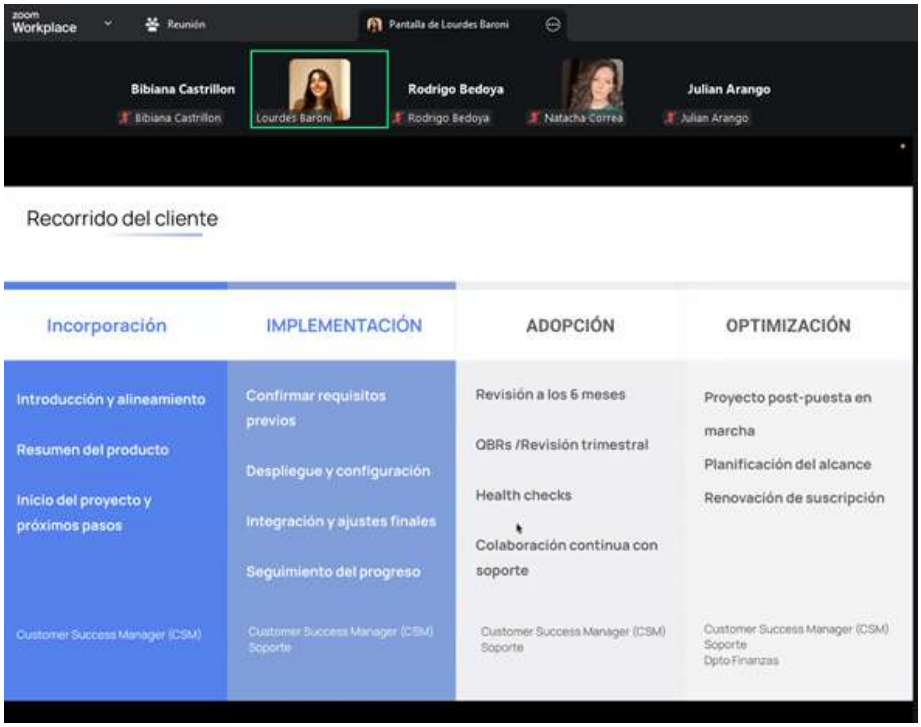

Status / Dashboard
Netgate Services And Support
Contract type pfSense TAC Professional
24 Hour SLA, Ticket
Support start 2026-04-27
Support end 2027-04-27
Support renewed 2026-04-27
Support status ACTIVE
NETGATE GLOBAL SUPPORT TAC PROFESSIONAL
Thank you for choosing a Netgate Global Support TAC PROFESSIONAL support subscription. Our 24/7 worldwide team of support engineers is the most qualified to diagnose your issue and resolve it quickly, from the branch office to enterprise — on-premises to the cloud. For non-critical issues, a ticket is appreciated. Also, check out the NETGATE RESOURCE LIBRARY for videos, documentation, and more!
Upgrade Your Support
Open a Support Request
Netgate Global Support FAQ
Official pfSense Training by Netgate
Netgate Professional Services
Visit Netgate.com
For critical support needs, please call 512-646-4100. You MUST have your Netgate Device ID (NDI) from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place.
System Information
Name PFS2.cdavgov.local
User admin@192.168.10.129 (Local Database)
System Netgate pfSense Plus
Serial: 2M281403J9
Netgate Device ID: f6c807effc54c628b22d
BIOS Vendor: HP

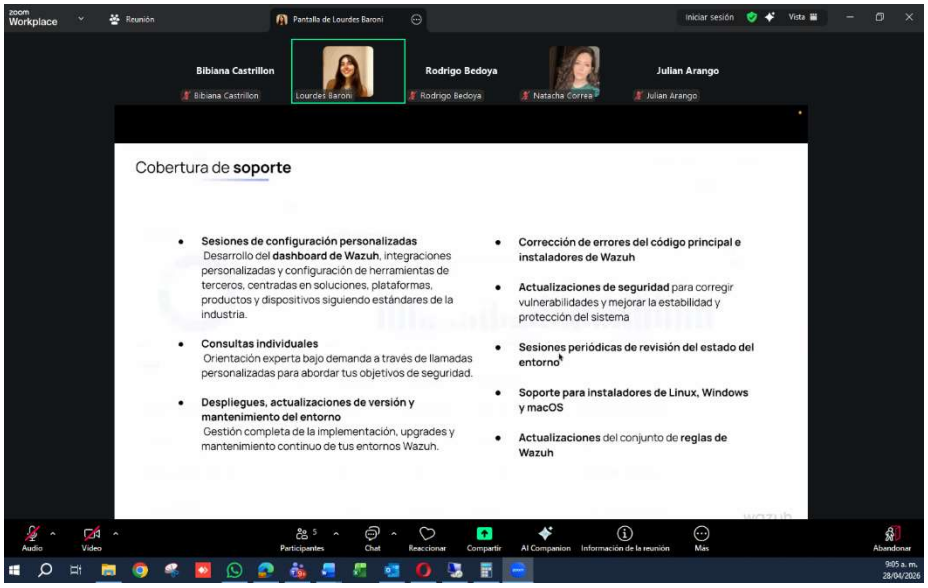
- **PFS-3**



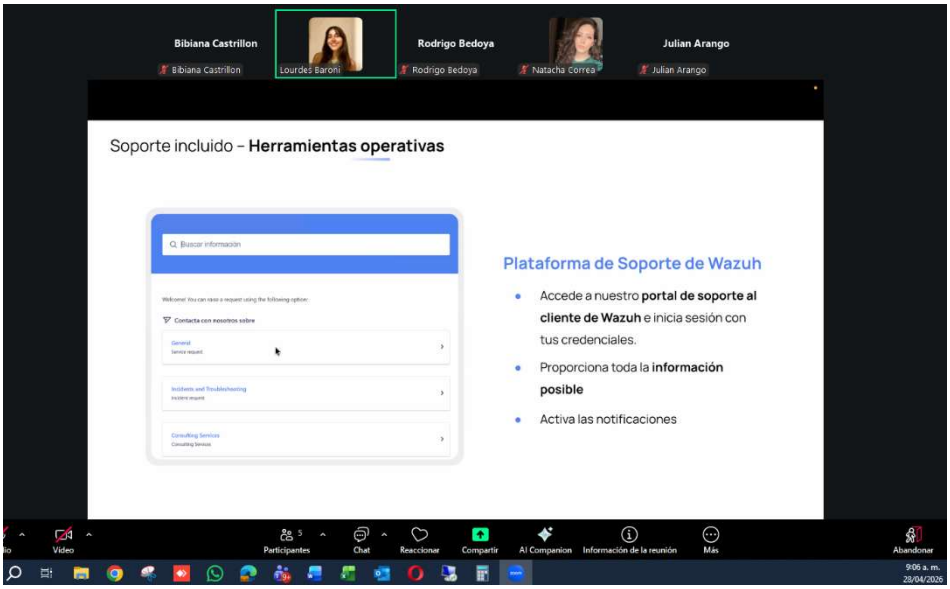

- **Wazuh:**

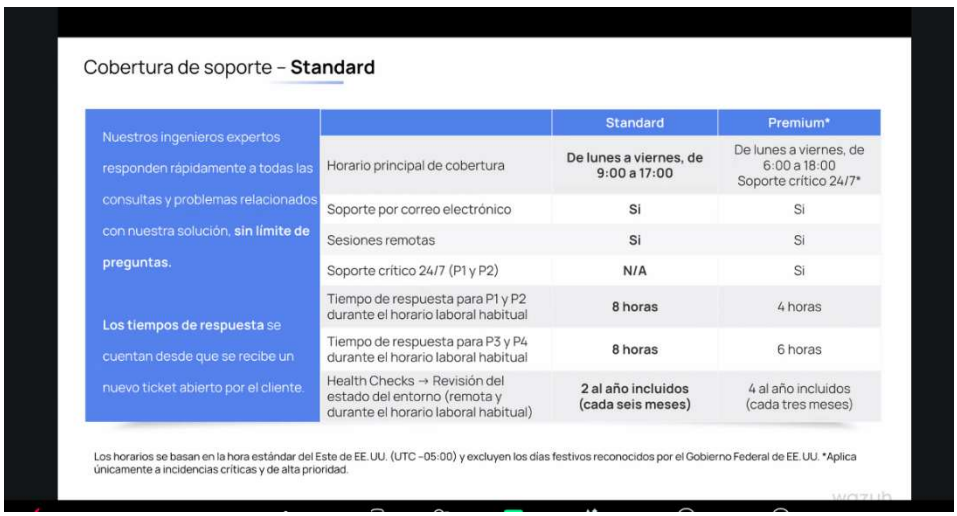
  En la reunión de onboarding, en la cual se revisó el detalle de la suscripción, cómo contactar al equipo técnico y definición de los próximos pasos a seguir.

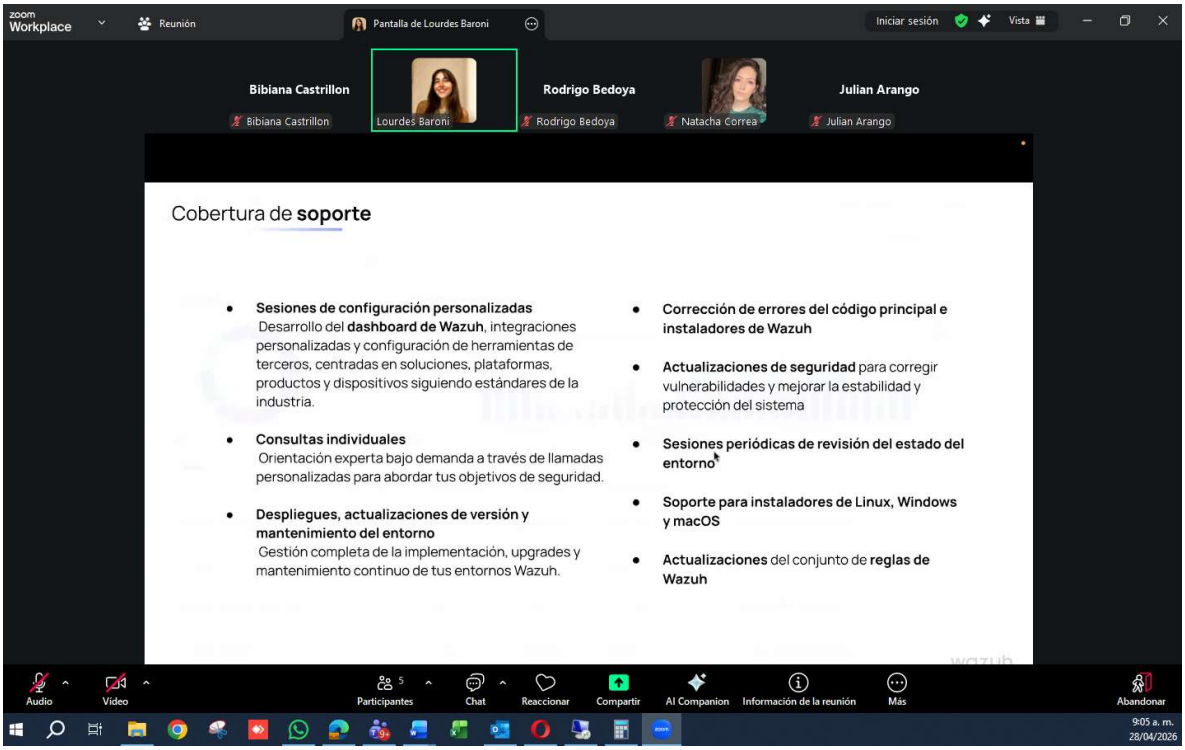

zoom Workplace
Reunión
Pantalla de Lourdes Baroni
Bibiana Castrillon
Rodrigo Bedoya
Julian Arango
Lourdes Baroni
Natacha Correa
Recorrido del cliente
Incorporación
IMPLEMENTACIÓN
ADOPCIÓN
OPTIMIZACIÓN
Introducción y alineamiento
Resumen del producto
Inicio del proyecto y próximos pasos
Confirmar requisitos previos
Despliegue y configuración
Integración y ajustes finales
Seguimiento del progreso
Revisión a los 6 meses
QBRs /Revisión trimestral
Health checks
Colaboración continua con soporte
Proyecto post-puesta en marcha
Planificación del alcance
Renovación de suscripción
Customer Success Manager (CSM)
Customer Success Manager (CSM)
Soporte
Customer Success Manager (CSM)
Soporte
Customer Success Manager (CSM)
Soporte
Dpto Finanzas

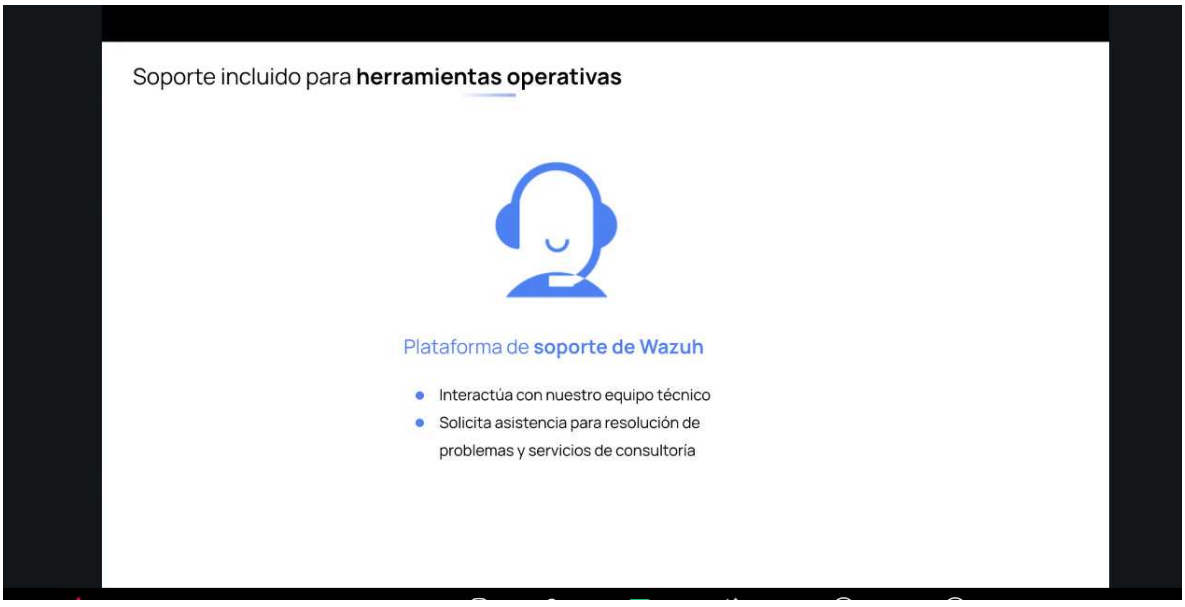

zoom Workplace
Reunión
Pantalla de Lourdes Baroni
Iniciar sesión
Vista
Bibiana Castrillon
Rodrigo Bedoya
Julian Arango
Lourdes Baroni
Natacha Correa
Cobertura de soporte
Sesiones de configuración personalizadas
Desarrollo del dashboard de Wazuh, integraciones personalizadas y configuración de herramientas de terceros, centradas en soluciones, plataformas, productos y dispositivos siguiendo estándares de la industria.
Consultas individuales
Orientación experta bajo demanda a través de llamadas personalizadas para abordar tus objetivos de seguridad.
Despliegues, actualizaciones de versión y mantenimiento del entorno
Gestión completa de la implementación, upgrades y mantenimiento continuo de tus entornos Wazuh.
Corrección de errores del código principal e instaladores de Wazuh
Actualizaciones de seguridad para corregir vulnerabilidades y mejorar la estabilidad y protección del sistema
Sesiones periódicas de revisión del estado del entorno
Soporte para instaladores de Linux, Windows y macOS
Actualizaciones del conjunto de reglas de Wazuh
Audio
Video
Participantes
Chat
Reaccionar
Compartir
AI Companion
Información de la reunión
Más
Abandonar
9:05 a. m.
28/04/2026

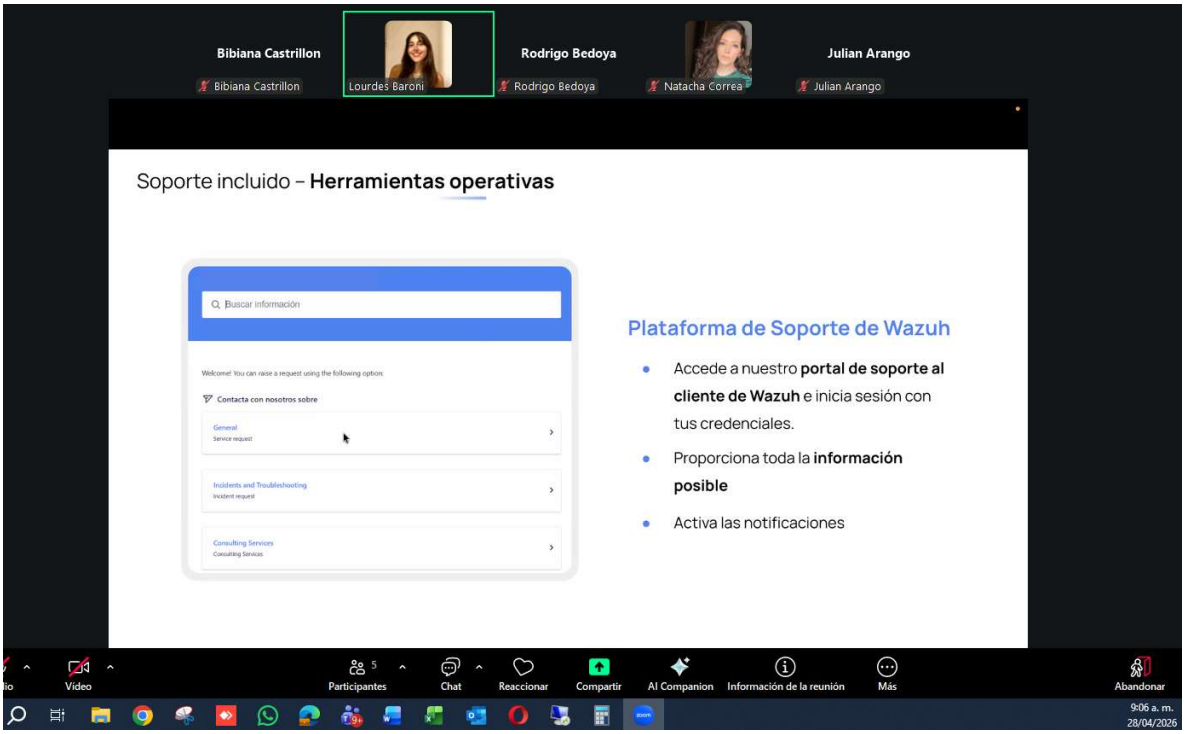

Soporte incluido para herramientas operativas
Plataforma de soporte de Wazuh
Interactúa con nuestro equipo técnico
Solicita asistencia para resolución de problemas y servicios de consultoría

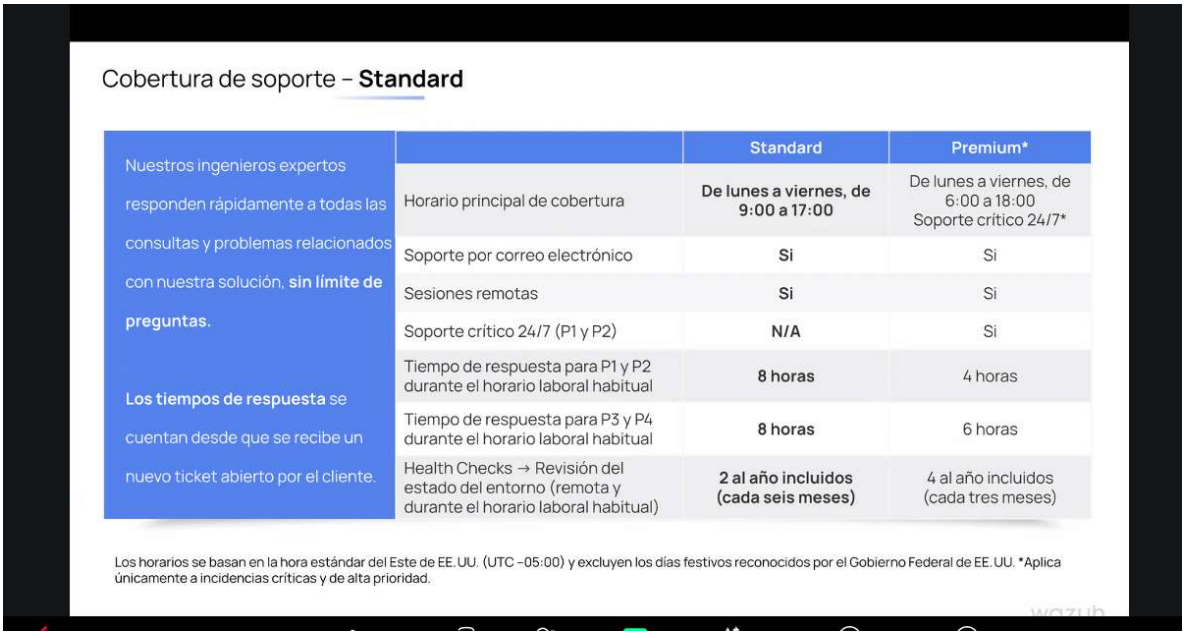

Bibiana Castrillon
Rodrigo Bedoya
Julian Arango
Soporte incluido – Herramientas operativas
Plataforma de Soporte de Wazuh
Accede a nuestro portal de soporte al cliente de Wazuh e inicia sesión con tus credenciales.
Proporciona toda la información posible
Activa las notificaciones

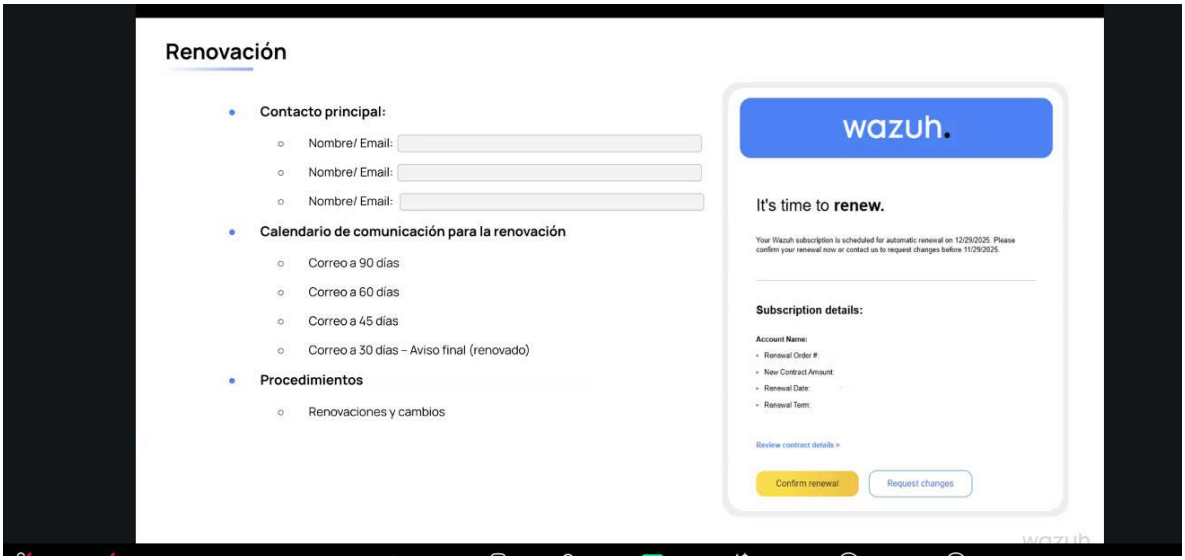

Cobertura de soporte – Standard
Nuestros ingenieros expertos responden rápidamente a todas las consultas y problemas relacionados con nuestra solución, sin límite de preguntas.
Los tiempos de respuesta se cuentan desde que se recibe un nuevo ticket abierto por el cliente.
Standard
Premium*
Horario principal de cobertura
De lunes a viernes, de 9:00 a 17:00
De lunes a viernes, de 6:00 a 18:00 Soporte crítico 24/7*
Soporte por correo electrónico
Sí
Sí
Sesiones remotas
Sí
Sí
Soporte crítico 24/7 (P1 y P2)
N/A
Sí
Tiempo de respuesta para P1 y P2 durante el horario laboral habitual
8 horas
4 horas
Tiempo de respuesta para P3 y P4 durante el horario laboral habitual
8 horas
6 horas
Health Checks → Revisión del estado del entorno (remota y durante el horario laboral habitual)
2 al año incluidos (cada seis meses)
4 al año incluidos (cada tres meses)
Los horarios se basan en la hora estándar del Este de EE.UU. (UTC -05:00) y excluyen los días festivos reconocidos por el Gobierno Federal de EE.UU. *Aplica únicamente a incidencias críticas y de alta prioridad.


zoom Workplace
Reunión
Pantalla de Lourdes Baroni
Iniciar sesión
Vista
Bibiana Castrillon
Rodrigo Bedoya
Julian Arango
Lourdes Baroni
Natacha Correa
Cobertura de soporte
Sesiones de configuración personalizadas
Desarrollo del dashboard de Wazuh, integraciones personalizadas y configuración de herramientas de terceros, centradas en soluciones, plataformas, productos y dispositivos siguiendo estándares de la industria.
Consultas individuales
Orientación experta bajo demanda a través de llamadas personalizadas para abordar tus objetivos de seguridad.
Despliegues, actualizaciones de versión y mantenimiento del entorno
Gestión completa de la implementación, upgrades y mantenimiento continuo de tus entornos Wazuh.
Corrección de errores del código principal e instaladores de Wazuh
Actualizaciones de seguridad para corregir vulnerabilidades y mejorar la estabilidad y protección del sistema
Sesiones periódicas de revisión del estado del entorno
Soporte para instaladores de Linux, Windows y macOS
Actualizaciones del conjunto de reglas de Wazuh
Audio
Vídeo
Participantes
Chat
Reaccionar
Compartir
AI Companion
Información de la reunión
Más
Abandonar
9:05 a. m.
28/04/2026

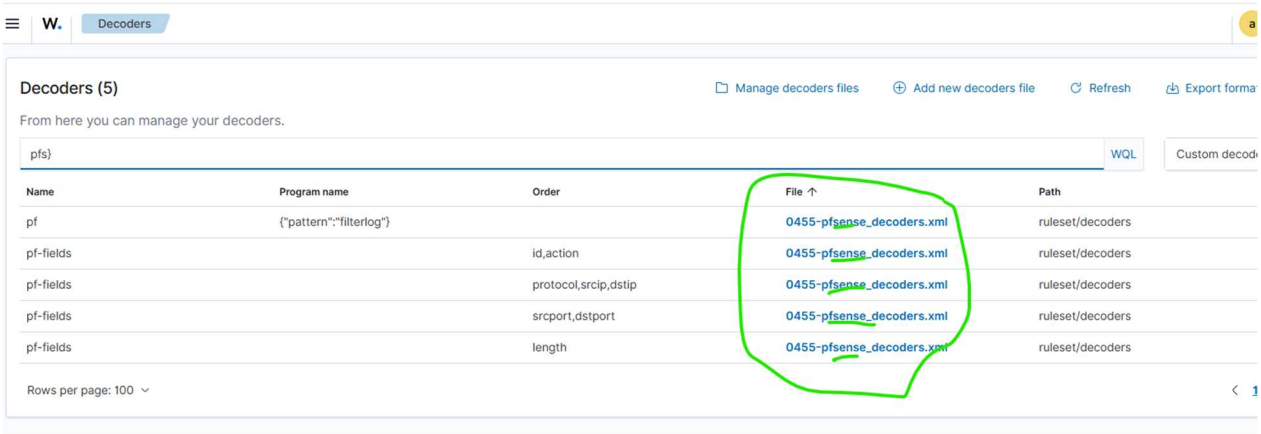

Soporte incluido para herramientas operativas
Plataforma de soporte de Wazuh
Interactúa con nuestro equipo técnico
Solicita asistencia para resolución de problemas y servicios de consultoría


Bibiana Castrillon
Lourdes Baroni
Rodrigo Bedoya
Natacha Correa
Julian Arango
Soporte incluido – Herramientas operativas
Buscar información
Welcome! You can raise a request using the following option:
Contacta con nosotros sobre
General
Service request
Incidents and Troubleshooting
Incident request
Consulting Services
Consulting Services
Plataforma de Soporte de Wazuh
Accede a nuestro portal de soporte al cliente de Wazuh e inicia sesión con tus credenciales.
Proporciona toda la información posible
Activa las notificaciones
Video
Participantes
Chat
Reaccionar
Compartir
AI Companion
Información de la reunión
Más
Abandonar
9:06 a. m.
28/04/2026

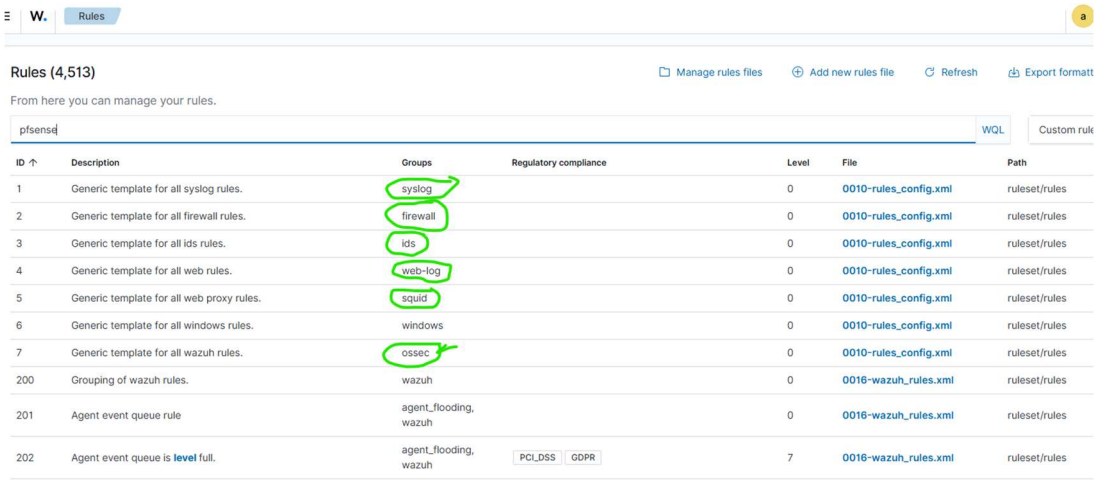

Cobertura de soporte – Standard
Nuestros ingenieros expertos responden rápidamente a todas las consultas y problemas relacionados con nuestra solución, sin límite de preguntas.
Los tiempos de respuesta se cuentan desde que se recibe un nuevo ticket abierto por el cliente.
Standard
Premium*
Horario principal de cobertura
De lunes a viernes, de 9:00 a 17:00
De lunes a viernes, de 6:00 a 18:00 Soporte crítico 24/7*
Soporte por correo electrónico
Si
Si
Sesiones remotas
Si
Si
Soporte crítico 24/7 (P1 y P2)
N/A
Si
Tiempo de respuesta para P1 y P2 durante el horario laboral habitual
8 horas
4 horas
Tiempo de respuesta para P3 y P4 durante el horario laboral habitual
8 horas
6 horas
Health Checks → Revisión del estado del entorno (remota y durante el horario laboral habitual)
2 al año incluidos (cada seis meses)
4 al año incluidos (cada tres meses)
Los horarios se basan en la hora estándar del Este de EE.UU. (UTC −05:00) y excluyen los días festivos reconocidos por el Gobierno Federal de EE.UU. *Aplica únicamente a incidencias críticas y de alta prioridad.




- Se evidencia que se crearon los decodificadores para el sistema PFSense de Netgate, como lo ilustra la imagen siguiente:




- Se evidencia que quedo apto para recibir alertas de los siguientes módulos del netgate Pfsense




| ID | Description | Groups | Regulatory compliance | Level | File | Path |
|---|---|---|---|---|---|---|
| 1 | Generic template for all syslog rules. | syslog | | 0 | 0010-rules_config.xml | ruleset/rules |
| 2 | Generic template for all firewall rules. | firewall | | 0 | 0010-rules_config.xml | ruleset/rules |
| 3 | Generic template for all ids rules. | ids | | 0 | 0010-rules_config.xml | ruleset/rules |
| 4 | Generic template for all web rules. | web-log | | 0 | 0010-rules_config.xml | ruleset/rules |
| 5 | Generic template for all web proxy rules. | squid | | 0 | 0010-rules_config.xml | ruleset/rules |
| 6 | Generic template for all windows rules. | windows | | 0 | 0010-rules_config.xml | ruleset/rules |
| 7 | Generic template for all wazuh rules. | ossec | | 0 | 0010-rules_config.xml | ruleset/rules |
| 200 | Grouping of wazuh rules. | wazuh | | 0 | 0016-wazuh_rules.xml | ruleset/rules |
| 201 | Agent event queue rule | agent_flooding, wazuh | | 0 | 0016-wazuh_rules.xml | ruleset/rules |
| 202 | Agent event queue is level full. | agent_flooding, wazuh | PCI_DSS GDPR | 7 | 0016-wazuh_rules.xml | ruleset/rules |

- Se evidencia que ya se están colectando alertas en el SIEM Wazuh mediante los decoders y reglas que fueron parametrizadas para detecciones correlacionadas de manera específicas y personalizadas.




En este caso anterior se ve que provienen del **PFS1** que es el **firewall** principal de la entidad.

## 4. Próximos Pasos

- Continuar con el monitoreo mensual y reporte de estabilidad.
- Mantener actualizados los componentes de seguridad y virtualización.

**Informe elaborado por:** Julian Arango



**Informe revisado y autorizado por:** Bibiana Castrillón

SOLUCIONES EN SEGURIDAD INFORMÁTICA
**Julian Andrés Arango Pineda**
**Soporte Técnico**
Email: ingenieroti@segurinfo.co
Usuario Skype: ingenieroti_1
Teléfono: (574) 4445088 Ext **1010** - Celular: (57) **350 6530859**
Carrera 79A No 53B-116 Int 101 Medellín – Colombia
Visita nuestra página www.**segurinfo.co/**